Please cite to this location: http://www.law.stanford.edu/library/biblio/rufus.pdf

Feel free to contact the author at rufus.pichler@stanfordalumni.org

# *TRUST AND RELIANCE—ENFORCEMENT AND COMPLIANCE: ENHANCING CONSUMER CONFIDENCE IN THE ELECTRONIC MARKETPLACE*

A THESIS

SUBMITTED TO THE

STANFORD PROGRAM IN INTERNATIONAL LEGAL STUDIES

AT THE STANFORD LAW SCHOOL,

STANFORD UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

JURIDICAL SCIENCES MASTER

By

Rufus Pichler

May 2000

# ABSTRACT

Consumers will not engage in impersonal exchange unless they either *trust* the merchant they are dealing with and believe that everything will go alright or they can comfortably *rely* on a third party to effectively afford them redress if things go wrong. Trust and reliance, which are to a large extent grounded on expected compliance and effective enforcement, are two distinct components of consumer confidence. This paper discusses why traditional bases for trust and reliance are no longer effective in the electronic marketplace. It argues that new institutions will emerge to enhance trust and reliance, namely information intermediaries and payment intermediaries, respectively. Of these two options, reliance mechanisms that can guarantee cheap and effective enforcement of consumer rights ultimately appear to be the more efficient approach to overcome the existing lack of consumer confidence.

The paper shows that some of these reliance mechanisms have developed in the market and it points out the crucial role of payment intermediaries in *every* online transaction. From a policy perspective it suggests to leverage this role and to consider addressing payment intermediaries by introducing comprehensive chargeback regimes that could guarantee effective consumer redress if something goes wrong in the transaction between a merchant and a consumer.

In their “Framework for Global Electronic Commerce” Bill Clinton and Albert Gore have emphasized that “consumers must have confidence ... that they will get what they pay for, and that recourse or redress will be available if they do not.”

Chargeback mechanisms appear to be a tool that can guarantee the latter. Therefore the paper argues that they are an approach worth pursuing in order to overcome “the global enforcement challenge” presented by the new online marketplace.

# PREFACE

First, I wish to thank the faculty of Stanford Law School, particularly Carey Heckman and Rogelio Perez-Perdomo, who have provided valuable suggestions and comments on previous drafts of this thesis. Stanford University in the heart of Silicon Valley is probably the most stimulating environment in the world for working on a topic related to electronic commerce. In such an environment it is difficult to acknowledge everybody who influenced the thinking that is expressed in this paper. To name a few though, I want to mention Peggy Radin, Mitch Polinsky, and Paul Goldstein. Their courses at Stanford Law School were great fun and provided numerous invaluable suggestions for my work.

I also owe thanks to my parents and the Studienstiftung des Deutschen Volkes whose financial support has helped to make this research possible and to Kate DeBoer who, among other things, directed me to the best Bed and Breakfast in Sonoma Valley when I needed to get out of here.

Finally, I want to express my gratitude to the staff of the Stanford University libraries, particularly the Robert Crown Law Library. Researchers can’t wish for better support than what I have experienced here.

# CONTENTS

I. Introduction ..... 1

II. The Online-Marketplace: Shaking the Foundations of Consumer Confidence ..... 8

A. Some Characteristics and Risks of Distance Transactions ..... 9

1) Security and Consumer Fraud ..... 13

2) Merchant Fraud and Consumer Redress ..... 23

B. What is “Consumer Confidence”? ..... 32

1) Trust and Reliance ..... 34

a) Trust ..... 35

b) Reliance ..... 44

c) Some Economics of Trust and Reliance ..... 46

2) Enforcement and Compliance ..... 51

C. Enforcement and Compliance in the Online-Marketplace ..... 54

1) Third Party Enforcement ..... 56

a) State Enforcement ..... 57

aa) The Federal Trade Commission and the Attorneys General ..... 60

α) Enforcement Efforts Regarding Electronic Commerce ..... 66

β) The Limits of State Enforcement and Their Implications for Consumer Reliance ..... 69

αα) Limited Enforcement ..... 70

ββ) Limited Reliance ..... 75

bb) The European Approach and Criminal Proceedings ..... 79

b) Court Enforcement ..... 81

aa) Suits Brought by Individual Consumers ..... 82

α) Some Economics of Consumer Litigation ..... 82

αα) Benefits ..... 83

ββ) Costs ..... 87

β) "The Consumer's Dilemma" ..... 89

bb) Rights to Sue for Consumer Organizations ..... 92

α) Collective Interests of Consumers ..... 94

β) Individual Interests of Consumers ..... 96

c) Organization Enforcement and Codes of Conduct (Self-Regulation) ..... 97

aa) Historic Examples of Successful Industry Self-Regulation ..... 101

bb) It's a Different World Online—The Failure of Self-Regulation as a Basis for Consumer Reliance ..... 104

d) Informal Enforcement of Social Norms ..... 109

2) Compliance ..... 112

a) Experience (Bilateral Reputation Mechanism) ..... 113

b) Reputation (Multilateral Reputation Mechanism) ..... 115

c) ... And Those Who Don't Care ..... 119

D. From Compliance to Trust? ..... 121

1) Information ..... 122

2) Time ..... 125

3) Investment and Branding ..... 126

E. Who Gets Left Behind? ..... 132

F. Summary—The Need for New Institutions ..... 138

III. Enhancing Consumer Confidence: The Rise of New External Institutions. 141

A. New Institutions to Foster Trust—Information Intermediaries ..... 142

1) The Approaches ..... 143

a) BBBOnline Reliability Program ..... 143

b) CPA WebTrust ..... 144

c) Bizrate, eComplaints, and e-Rating ..... 145

2) The Limits ..... 147

B. Reliance on New Enforcement Institutions—The Crucial Role of Payment Intermediaries ..... 150

1) Market Approaches ..... 151

a) Escrows ..... 151

b) "Blue," Shopping Guarantees, and Insurance ..... 153

2) A Policy Perspective—Addressing Payment Intermediaries and Introducing Chargeback Mechanisms ..... 154

a) Chargebacks in U.S. Credit Card Regulation ..... 154

b) Chargebacks as a General Enforcement Model ..... 155

IV. Conclusions ..... 158

# I. INTRODUCTION

"Despite all of the sound and fury, business to consumer commercial online transactions are but in their earliest stages." Just over a third of Internet users report that they actually make purchases online. These are some of the key findings of a recent study by the Stanford Institute for the Quantitative Study of Society.[1] This paper will argue that this relatively poor performance of business-to-consumer electronic commerce is due to a lack of consumer confidence and that new institutions are needed to overcome this deficit.

Various private and public institutions hopelessly disagree about how much wealth electronic commerce can potentially generate. According to one comparison the 1995 estimates of e-commerce revenues in the year 2000 ranged from $580 *million* to $775 *billion*[2]—more than 1000 times the lower estimate (a discrepancy that presumably accounts for the use of the term

---

[1] *See* Norman H. Nie & Lutz Erbring, Stanford Institute for the Quantitative Study of Society, *Internet and Society: A Preliminary Report* 4 (Feb. 17, 2000) <http://www.stanford.edu/group/siqss/Press_Release/Preliminary_Report.pdf>. *See also* SIQSS, *Internet Study* (last modified Feb. 18, 2000) <http://www.stanford.edu/group/siqss/Press_Release/internetStudy.html> (providing background information on the study); Kathleen O'Toole, *Study takes early look at social consequences of Net use*, STANFORD REPORT [ONLINE] (Feb. 16, 2000) <http://www.stanford.edu/dept/news/report/news/february16/internetsurvey-216.html> (reporting on the study).

[2] *See* OECD, Committee for Information, Computer and Communications Policy, *Measuring Electronic Commerce*, OCDE/GD(97)185, table 2 at 24-25 (containing comprehensive tables with a comparison of various electronic commerce estimates by Hambrecht & Quest, Forrester Research and many others). *See also* OECD, THE ECONOMIC AND SOCIAL IMPACT OF ELECTRONIC COMMERCE: PRELIMINARY FINDINGS AND RESEARCH AGENDA table 1.1 at 27 (1999) [hereinafter OECD, THE IMPACT OF ELECTRONIC COMMERCE] (presenting yet different figures).

"guesstimate" in similar contexts).[3] Virtually every source provides different figures. Some forecast that the one trillion-dollar threshold will be crossed by 2003.[4] In fact, it is even far from clear how to define,[5] let alone how to accurately measure electronic commerce.[6] This probably accounts for the fact that not only can one find significant differences in future estimates, but also in ex post statistics on electronic commerce returns.[7] According to one comparison the

---

[3] *See, e.g.*, Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 68 (1996).

[4] *See* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, TOWARDS DIGITAL EQUALITY, SECOND ANNUAL REPORT at iii, 7 (1999), available at <http://www.ecommerce.gov/ecomrce.pdf> [hereinafter WORKING GROUP II]. *See also* U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998), available at <http://www.ecommerce.gov/EmergingDig.pdf> [hereinafter DIGITAL ECONOMY I]; U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY II (1999), available at <http://www.ecommerce.gov/ede/ede2.pdf> [hereinafter DIGITAL ECONOMY II]; U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT (1998), available at <http://www.doc.gov/ecommerce/E-comm.pdf> [hereinafter WORKING GROUP I] (all providing measurements and estimates of electronic commerce as well as a general and comprehensive analysis of the digital economy).

[5] For a good overview on various definitions of Electronic Commerce see OECD, *Measuring Electronic Commerce, supra* note 2, at 6 Box A, 19 Figure 1. The OECD's own working definition of electronic commerce in that paper is that of "commercial transactions occurring over open networks, primarily the Internet." *See id.* at 9.

[6] The OECD has taken on the task to develop "E-commerce statistics that are internationally comparable, and therefore based on a common set of definitions and a common measurement framework for e-commerce." (*See* OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on Indicators for the Information Society, *Defining and Measuring E-Commerce: A Status Report*, DSTI/ICCP/IIS(99)4/FINAL at 6 (Oct. 7, 1999). *See also* OECD, *Measuring Electronic Commerce*, *supra* note 2; OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on the Information Economy, *Measuring Electronic Commerce: International Trade in Software*, DSTI/ICCP/IE(98)3/FINAL (April 27, 1998) [hereinafter OECD, *Measuring Trade in Software*]. Meaningful measurement of the Digital Economy is also one of the U.S. government's primary objectives, *see* WORKING GROUP II, *supra* note 4, at vi, 23-25 (referring to president Clinton's 1998 directive on electronic commerce; this Directive has led the reports DIGITAL ECONOMY I and II, *supra* note 4).

One of the most influential factors is, whether or not the estimates distinguish between business-to-business and business-to-consumer e-commerce. The volume of the first greatly exceeds that of the latter, *see, e.g.*, OECD, *Measuring Electronic Commerce, supra* note 2, at 3. *See also infra* note 10.

[7] According to OECD, *Measuring Electronic Commerce, supra* note 2, at 7, "[a]ll estimates of electronic commerce activity are based on revenues, not value added, ....". *See also* Maryann

1995 figures for actual electronic commerce revenues ranged from $45 million to $1.17 billion.[8]

In one regard, however, everybody seems to agree:[9] It should be more. Indeed, some say that e-commerce—and one should be more specific and say *business-to-consumer* e-commerce[10]—so far has not met the expectations at all,[11] at least not in all parts of the world.[12] The more optimistic ones concede a great danger

---

Jones Thompson, *Spotlight: Why E-commerce Forecasters Don't Get It "Right"*, The Standard (Mar. 1, 1999) <http://www.thestandard.com/research/metrics/display/0,2799,9881,00.html>.

[8] *See* OECD, *Measuring Electronic Commerce, supra* note 2, table 2 at 25.

[9] With the exception, of course, of those who generally oppose and regret the commercialization of the Internet (particularly the World Wide Web), wishing to return to old times in which the net was a social rather than a commercial space and the users were a more or less homogenous group sharing common values. For good accounts of how "the net used to be" (or at least was perceived to be) see, e.g., CLIFFORD STOLL, SILICON SNAKE OIL (1995); SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET (1995); HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993); MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY 342 *passim* (1996) and the various articles in HIGH NOON ON THE ELECTRONIC FRONTIER (Peter Ludlow ed., 1996).

The process of commercialization has been vividly described by Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 Jurimetrics J. 1, 8 (1994) as "the [then] relatively recent influx of 'immigrants' from the real world who are arriving in droves in the belief that cyberia's highways are paved with gold."

[10] The distinction between business-to-business and business-to-consumer e-commerce is vital, since both segments are driven by different factors and face a number of completely different barriers. For a good summary of the different issues each of these segments is facing see OECD, THE IMPACT OF ELECTRONIC COMMERCE, *supra* note 2, at 37, 42 (listing drivers and inhibitors of business-to-business and business-to-consumer e-commerce, respectively). *See also* DIGITAL ECONOMY I, *supra* note 4, at 12 *passim*, 24 *passim*; WORKING GROUP II, *supra* note 4, at 5-8; OECD, *Measuring Electronic Commerce, supra* note 2, at 11-13 (all emphasizing the distinction between the two segments); DIGITAL ECONOMY II, *supra* note 4, 10-12 (speaking of "retail e-commerce" and business-to-business e-commerce).

[11] Of course one has to take into account, that some of the estimates (*see supra* note 2) seemed highly exaggerated in the first place. Those that refer to lower estimates in the first place found that the expectations for 2000 (in this case being $7 billion) were exceeded in 1998, *see* WORKING GROUP II, *supra* note 4, at 6.

[12] *See, e.g.*, DIGITAL ECONOMY II, *supra* note 4, at 6 (pointing out that "[c]ompared with businesses and consumers overseas, U.S. businesses and consumers appear to have a greater desire and willingness to transact business online."). *See also* Dermot McGrath, *When 'E' Stands for Europe*,

that expectations will not be met in the future.[13] Everyone even seems to agree on the principal reason that to date has prevented e-commerce from living up to its full potential: a *lack of consumer trust and confidence* in the electronic marketplace. This concern is expressed by all major policy papers and private sector analyses. Consequently, these analyses define establishing enhanced consumer confidence as their number one goal with regard to the further development of electronic commerce. The following passage from the U.S. Government's Framework for Global Electronic Commerce is exemplary[14] for the prevailing view:

---

COMPUTERWORLD, Sept.6, 1999, at 52 ("Europeans are more reluctant than Americans to buy online, ....").

[13] *See* WORKING GROUP II, *supra* note 4, at iv ("The robust projections for the growth of electronic commerce are unlikely to hold true unless online consumers can shop the Web with confidence.").

[14] In additions to the sources cited *infra* notes 16, 17, and 20 *see also* The National Advisory Council on Consumer Affairs (Australia), *Consumer Protection in Electronic Commerce* 2 (April 1998) ("foster public confidence in the electronic marketplace"), available online at <http://www.treasury.gov.au/publications/ConsumerAffairs/ElectronicCommercePublications/ConsumerProtectionInElectronicCommerce-PrinciplesAndKeyIssues/index.asp>; Global Information Networks, Ministerial Conference Bonn 6-8 July 1997, *Ministerial Declaration* para. 29 (visited Aug. 17, 00) <http://www2.echo.lu/bonn/final.htm> [hereinafter *Bonn Declaration*] ("Ministers recognise that it is crucial to build trust and confidence in Global Information Networks ...."); Consumers International, *Consumers@shopping: An international comparative study of electronic commerce* 7 (1999), available online at <http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf> ("If consumers are to take full advantage of the global shopping mall theoretically offered by the Internet, they must feel confident of receiving a consistent standard of consumer protection wherever they shop."); OECD, Directorate for Science, Technology and Industry, Committee on Consumer Policy, *Consumer Protection in the Electronic Marketplace*, DSTI/CP(98)13/FINAL at 4 (Dec. 22, 1998) ("Direct business-to-consumer electronic commerce will not reach its full potential until consumers are assured that the online environment is a safe and predictable place for them to do business. .... Working together, governments, businesses and consumer representatives can help to enhance consumer confidence in electronic commercial transactions while encouraging the development of the global marketplace."); OECD, Directorate for Science, Technology and Industry, *OECD Forum on Electronic Commerce: Report on the Forum, OECD, Paris, 12-13 October 1999*, SG/EC(99)12 at 6, 14 (Nov. 24, 1999) ("Users must gain confidence in the digital marketplace.", "Trust is central to any transaction, electronic or otherwise.").

> "In order to realize the commercial and cultural potential of the Internet, consumers must have confidence that the goods and services offered are fairly represented, that they will get what they pay for, and that recourse or redress will be available if they do not."[15]

Similarly, the European Commission stated that "[t]he first objective is to build trust and confidence."[16] Speaking for the private sector the Alliance for Global Business, representing business interest groups from around the world, has made detailed recommendations on "[b]uilding trust for users and consumers."[17] And according to the Global Business Dialogue on Electronic Commerce (GBDe)—characterizing itself as "an unprecedented world-wide collaboration among leading CEO's and board members of companies engaged in the field of electronic commerce"[18] and being characterized by the U.S. Government

---

[15] *See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE at III.8. (1997), available at <http://www.ecommerce.gov/framewrk.htm> [hereinafter FRAMEWORK]. *See also* WORKING GROUP I, *supra* note 4, at 27 (containing an almost identical formulation); WORKING GROUP II, *supra* note 4, at 17 ("Consumers must be confident that the goods and services offered online are fairly represented and the merchants with whom they are dealing—many of whom may be located in another part of the world—deliver their goods in a timely manner and are not engaged in illegal business practices such as fraud or deception. Consumer confidence also requires that consumers have access to fair and effective redress if they are not satisfied with some aspect of the transaction.").

[16] *See A European Initiative in Electronic Commerce*, COM(97)157 final para. 35.

[17] *See* Alliance for Global Business, *A Global Action Plan for Electronic Commerce: Prepared by Business with Recommendations for Governments* 20 *passim* (2d ed. 1999), available online at <http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/bizac_e.pdf> (identical with OECD Doc. SG/EC(99)6); (An earlier version of this paper was also submitted as a background document to the OECD Ministerial Conference in Ottawa, Canada, Oct. 7-9, 1998. *See* OECD, Directorate for Science, Technology and Industry, Steering Committee for the Ottawa Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce", *A Global Action Plan for Electronic Commerce Prepared by Business With Recommendations From* [sic!] *Governments*, SG/EC(98)11/REV2 (Oct. 5, 1998), available at <http://www.oecd.org//dsti/sti/it/ec/prod/sgec_11e.pdf>).

[18] Involved companies include NEC Corporation, DaimlerChrysler, The Walt Disney Company, Nortel Networks, Fujitsu Limited, EDS, Telefónica, Toshiba Corporation, and Deutsche Bank.

Working Group on Electronic Commerce as "an important new force for self-regulation and policy leadership"[19]—"[c]onsumer confidence is a key issue for the development of electronic commerce, and both business and governments have a responsibility to foster it."[20] Retailers, finally, see lack of consumer confidence "as their number one concern."[21]

In this paper I will look at the issue of consumer confidence in greater detail. The following section will summarize some of the characteristics and risks of distance transactions in general and of electronic commerce over the Internet in particular. This will help to more specifically identify possible reasons for consumers to feel uncomfortable about engaging in commercial transactions online. It will go on to define what "confidence", "trust", and similar terms actually mean, and it will argue for making an important distinction between "trust" and "reliance." This distinction is not made clearly enough in the existing literature, although it has important implications for the remedies that are suited to overcome the confidence problem. The section will analyze the grounds of trust and reliance, how they relate to enforcement and compliance, and why they are lacking in the online-environment. The section wil find that above all a lack of *initial* trust and reliance is likely to be a significant entry-barrier to the electronic marketplace.

---

[19] *See* WORKING GROUP II, *supra* note 4, at 12.

[20] *See* Global Business Dialogue on Electronic Commerce (GBDe), *The Paris Recommendations* (Sep. 13, 1999) (visited Aug. 17, 00) <http://www.gbd.org/conference/recommendations.html>.

[21] *See* Linda Leung, *Five per cent of all online transactions are fraudulent*, vnunet.com (Nov. 24, 1999) <http://www.vnunet.com/News/103736> (referring to a survey of 100 online retailers).

To this background part III will discuss different ways to enhance consumer confidence. It argues that new institutions will emerge to enhance trust and reliance, namely information intermediaries and payment intermediaries, respectively. Of these two options, reliance mechanisms that can guarantee cheap and effective enforcement of consumer rights ultimately appear to be the more efficient approach to overcome the existing lack of consumer confidence. It will emphasize the crucial role of payment intermediaries and it will in particular discuss the introduction of a comprehensive chargeback regime as a means to accelerate the development of business-to-consumer electronic commerce. Part IV will summarize the findings and offer some concluding remarks.

## II. THE ONLINE-MARKETPLACE: SHAKING THE FOUNDATIONS OF CONSUMER CONFIDENCE

People have been engaging in business transactions for a long time. Never before, however, have concerns about consumer confidence been subject to so much discussion.[22] In fact, every transaction requires some degree of confidence or trust.[23] So why is it that everybody seems to be *particularly* concerned about consumer confidence in the electronic marketplace? The reason for this is not, as I will lay out in more detail below, that electronic commerce requires more consumer confidence than other types of commercial transactions. It is rather that with regard to "traditional" transactions there have, over time, evolved some solid bases for consumer confidence. These bases, however, appear not to work very well with regard to online transactions. This part will analyze why.

---

[22] To be sure, as Cynthia Hardy et al., *Distinguishing Trust and Power in Interorganizational Relations: Forms and Façades of Trust*, *in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 64, 66 (Christel Lane & Reinhard Bachmann eds., 1998) point out, "the literature on trust is burgeoning and the topic has been considered by economists, psychologists, and sociologists, as well as management theorists." (Citations omitted). *See generally infra* note 149. But the emphasis on the need to foster *consumer confidence* in regard to online transactions puts a new twist on the discussion.

[23] *See, e.g.*, John Humphrey, *Trust and the Transformation of Supplier Relations in Indian Industry, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 214, 217 (arguing generally that "[t]he question of trust arises from the element of risk in economic transactions."); Partha Dasgupta, *Trust as a Commodity, in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 49 (Diego Gambetta ed., 1988) [hereinafter TRUST (Gambetta ed.)] ("Trust is central to all transactions ....").

## A. Some Characteristics and Risks of Distance Transactions

Online transactions, just like catalogue sales, mail orders, or telephone orders, are distance transactions.[24] All of these transactions share some common characteristics.[25] First, these transactions are non face-to-face transactions.[26] The parties therefore will often have no knowledge of the other's identity, age, or whereabouts. They do not get a personal impression nor can they assess gestures or body language.[27] Moreover, they might confront information deficiencies.[28] Since it is not possible to ask a salesperson at a physical place,

---

[24] Consequently all of the mentioned transactions fall within the scope of the Directive 97/7/EC of the European Parliament and of the Council on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19 [hereinafter Distance Contracts Directive]. According to art. 2(1) of the Directive, a distance contract basically consists of two elements: (1) the exclusive use of a means of distance communication before and for the formation of the contract and (2) an organized distance sales or service-provision scheme run by the supplier. A means of distance communication is defined in art. 2(4) as any means that is used for the conclusion of contracts between parties who are not simultaneously physically present at the same location. Annex I of the Directive contains a non-exhaustive list of such means, including printed matters, letters, catalogues, telephone, radio, electronic mail, fax, or television. The Directive thus applies to classic forms of distance selling such as catalogue sales, mail-order, telephone-order, or teleshopping, as well as to more recent developments, in particular e-commerce transactions over the Internet. *See* Rufus Pichler, *The Directive 97/7/EC of the European Parliament and of the Council on the Protection of Consumers in Respect of Distance Contracts: Theoretical and Practical Impacts on Transatlantic Electronic Commerce* II.B.1) (Dec. 22, 1999) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies).

[25] In some very important respects, however, online transactions are also distinct from the others. *See* detailed discussion *infra* II.C.

[26] *See also* Froomkin, *supra* note 3, at 68 *passim* (comparing differences between face-to-face sales, telephone sales, and Internet sales).

[27] *See also infra* note 190 and accompanying text.

[28] *See* Australian Competition & Consumer Commission, *The Global Enforcement Challenge: Enforcement of consumer protection laws in a global marketplace* Part II.2., at 7-10 (Aug. 1997) [hereinafter ACCC, *Enforcement Challenge*], available online at <http://www.accc.gov.au/docs/global/front.htm>. It is also one of the main objectives of the European Distance Contracts Directive to ensure sufficient consumer information, *see* Distance Contracts Directive, *supra* note 24, recitals para 11. See also the preceding Commission Recommendation 92/295/EEC of 7 April 1992 on Codes of Practice for the Protection of Consumers in Respect of Contracts Negotiated at a Distance (Distance Selling), 1992 O.J. (L 156) 21, which points out the necessity of sufficient consumer information and recommends suppliers to adopt a code of conduct with regard do distance sales.

the nature of a distant transaction might lead to insufficient information about the product, service, merchant, conditions of the contract, or other relevant factors. The consumer will generally not have an opportunity to see, examine, or test the product or to ascertain the service she is about to purchase before concluding the respective contract.[29] Nor will she get an impression of the merchant's shop or a feeling of comfort in regard to visible assets that might eventually allow recourse should things go wrong.[30] A second characteristic, much more of Internet transactions than of traditional remote business-to-consumer transactions like catalogue sales, mail or telephone orders, is that they are often international—the merchant's principal place of business being in one, the consumer's domicile in another country (so called cross-border transactions).[31] Third, and most importantly, distance transactions are characterized by the fact, that one party will typically have to perform prior to the other. An immediate on the spot exchange of product or service and money, as, for example, in a

---

[29] *See* Helmut Köhler, *Die Rechte des Verbrauchers beim Teleshopping (TV-Shopping, Internet-Shopping*), 1998 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 185, 186 (listing these and other risks related to distance shopping).

[30] *See* Froomkin, *supra* note 3, at 71. We will come back to this very important point when we talk about investment as a basis for trust, *see infra* II.D.3).

[31] *See, e.g.*, ACCC, *Enforcement Challenge, supra* note 28, at 1; *See* John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. 893, 912 (1999) (finding an increased volume of cross-border transactions). The fact that businesses selling online have immediate access to *international* markets without facing typical "offline-barriers" such as setting up a local marketing and distribution network is repeatedly emphasized as one of the major advantages of e-commerce. *See, e.g.*, Fred M. Greguras et al., *Software Marketing, Licensing and Distribution in Cyberspace*, 1 CYBERSPACE LAW. 4 (1996) ("The Internet provides software vendors with wide exposure, an inexpensive marketing channel, and access to international markets earlier than ever before."); OECD, *Measuring Trade in Software, supra* note 6, at 18-22 (giving estimates for international trade in digital products over the Internet).

physical store,[32] is impossible. This last characteristic makes the transaction risky, particularly for the party that has to perform in advance. She might fulfill her obligation just to learn later that the other party does not fulfill hers in return.[33] This *risk of prior performance* will be an important background to most of the rest of this paper.

In the broader context of possible barriers to the full development of e-commerce, however, it is important to note that the fear of fraud is only one of a variety of factors that can potentially impair the growth of e-commerce.[34] These factors include[35] economic, factual, and technological barriers, mainly the ease and cost of access to the Net,[36] the availability of broad band connections,[37] and of course the accessibility of the merchants' servers[38] as well as a satisfactory

---

[32] *See also* Froomkin, *supra* note 3, at 70 (stating that "in a face-to-face sale, there is no problem with moving value").

[33] Louis H. Bluhm, *Trust, Terrorism, and Technology*, 6 J. BUS. ETHICS 333, 338 (1987) expresses this words that are much more sophisticated: "In the marketplace, where the self-interest of one actor is likely to be advanced at the expense of another, there is an inherent fear that others will succumb to the temptation to misrepresent behavior and use deception in the exchange process."

[34] Besides the fact that ultimately consumers actually need to have an interest in the goods or services offered, which is, of course, by no means unique to e-commerce.

[35] *See also* United States Government, Electronic Commerce Policy, *Request for Public Comment on Legal Barriers to Electronic Commerce* (visited Aug. 17, 00) <http://osecnt13.osec.doc.gov/ecommerce/barriers.nsf>.

[36] *See, e.g.*, OECD, THE IMPACT OF ELECTRONIC COMMERCE, *supra* note 2, at 42.

[37] *See* DIGITAL ECONOMY II, *supra* note 4, at 7; WORKING GROUP II, *supra* note 4, at 3-17 (emphasizing the importance of high speed Internet access and summarizing the progress with regard to the respective presidential Directive).

[38] A study by Andersen Consulting found that 25 percent of attempted online purchases failed because the merchants' web sites could not take orders because they crashed, were blocked, were under construction, or were otherwise inaccessible. *See* Andersen Consulting, Press Release, *One Quarter of Attempted On-Line Holiday Purchases End in "No Sale"* (Dec. 20, 1999) <http://www.andersen.com/news/newsarchive/12.99/newsarchive_122099.html>.

handling of orders.[39] Whether they are charged at a flat rate or face a metered pricing structure for local phone calls or a flat or metered fee for Internet access through their Internet Service Provider (ISP) makes a difference with regard to how much time users spend online.[40] And the time users spend online, as does the available bandwidth which is responsible for download times[41] and contributes to the overall convenience of the "shopping experience",[42] relates directly to how much money they spend online.[43] Besides ease and cost of access, speed of transmission, and convenience sources frequently list psychological factors such as users' preference for the experience of buying products that they can see, feel, or try on in person[44] among possible factors slowing down the development of e-commerce. On the other hand, all these factors and a fear of *consumer* fraud[45] can obviously also deter merchants from selling online.

Neither a limited infrastructure nor individual preferences, however, but *concerns* seem to be the predominant inhibitor that accounts for a continuing wariness of a

---

[39] *See infra* note 123 (pointing to consumer's fears that their online holiday purchases will not arrive in time).

[40] *See* sources cited *supra* note 37.

[41] For a comparison of download times using different technologies see DIGITAL ECONOMY I, *supra* note 4, at 9.

[42] *See id. See also* OECD, THE IMPACT OF ELECTRONIC COMMERCE, *supra* note 2, at 42 (particularly pointing to the importance of convenience to users).

[43] *See id.* (referring to an ActivMedia study for "[t]he finding that the longer shoppers use the Internet, the more likely they are to buy on line ...."). *See also* Nie & Erbring, *supra* note 1, at 5.

[44] *See* DIGITAL ECONOMY I, *supra* note 4, at 45. *See also* OECD, *Measuring Trade in Software, supra* note 6, at 45 ("consumers' love for the 'look and feel' of the software box, ....").

[45] As opposed to merchant fraud, s*ee infra* II.A.1).

significant number of users to shop online. The top three concerns are privacy, security, and fraud.[46] Privacy, about which according to a 1998 poll 81 percent of American Internet users have significant concerns,[47] touches on many of the issues that will be discussed here. Particularly the question of *trust* is frequently addressed in regard to what users believe a merchant will or will not do with their personal data and how that influences their decision as to whether or not to transact with a particular merchant.[48] The scope of this paper, however, does not allow to discuss the problem of privacy further,[49] since it raises a whole set of different and complex issues. Instead I will focus on the two other main concerns: security and fraud.

### *1) Security and Consumer Fraud*

Security concerns, to the extent they are of interest here, are really just concerns about an anticipated fraud. Fraud can basically occur in two forms: It can be committed against the merchant, which I will call *consumer fraud*, or it can be

---

[46] *See, e.g.*, OECD, THE IMPACT OF ELECTRONIC COMMERCE, *supra* note 2, at 42; DIGITAL ECONOMY I, *supra* note 4, at 45; DIGITAL ECONOMY II, *supra* note 4, at 7; WORKING GROUP II, *supra* note 4, at iv; FRAMEWORK, *supra* note 15, at 11, 14, 19 (each listing some or all of these concerns among the barriers for e-commerce growth). *See also* Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 841-42 (1999) ("[M]any consumers continue to have little confidence in the ability of sellers to deliver goods and services without compromising the security of sensitive information.").

[47] *See* WORKING GROUP I, *supra* note 4, at 16. The awareness and the concerns about privacy seem to have been rising constantly before and since then, *see, e.g.*, Roland Vogl, *The EU—U.S. Privacy Debate* (May 2000) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies) and the sources cited there.

[48] Note, however, that not all of the solutions discussed and proposed herein are applicable to the privacy problem.

[49] For a thorough and recent discussion of privacy issues in cyberspace see Symposium, *Cyberspace and Privacy—A New Legal Paradigm*, 52 STAN. L. REV. (forthcoming 2000).

committed against the consumer, which I will consequently refer to as *merchant fraud*.[50] Concerns about the security of network communications or the network infrastructure, mainly about third parties getting access to data that they are not supposed to get access to, typically just anticipate a third type of fraud at a later stage—*third party fraud*. This is quite obvious if one agrees with the basic assumption that merely getting access to secret data normally[51] is not the ultimate end of the intruder's conduct. Typically she wants to use this data to his own advantage, i.e. committing fraud against a merchant, a consumer or some other institution such as a bank or credit card company. Who exactly the ultimate victim of third party fraud will be, depends on the legal risk allocation among the parties that are involved. In the case of an unauthorized use of a credit card, for example, the victim could be the card issuer, the merchant who accepts the card for payment, or the cardholder, depending on how the parties and the law allocate this risk under the given circumstances.[52]

---

[50] *See infra* II.A.2). Note that the use of the terminology varies. Consumer fraud and merchant fraud means the opposite when one does not use it for fraud *by* consumers or merchants (as it is used here), but for fraud committed *against* consumers or merchants (as it is used, for example, in Federal Trade Commission, Report, *Fighting Consumer Fraud: New Tools of the Trade* (April 1998) <http://www.ftc.gov/reports/fraud97/fraud97.pdf> [hereinafter FTC, *New Tools of the Trade*] or in Federal Trade Commission, Report, *Fighting Consumer Fraud: The Challenge and the Campaign* (Jan. 1997) <http://www.ftc.gov/reports/Fraud/index.htm> [hereinafter FTC, *The Challenge and the Campaign*].

[51] I will leave aside the phenomenon of the honorable hacker, whose only goal it is to find security leaks in the system and who doesn't pursue any self-interest. I will leave this phenomenon aside for two reasons: First, because I believe these people to be an endangered species, and more importantly, because of the fact that when people do have *concerns* about security they will normally think about those, who will actually misuse the data they discovered. For an overview on hackers and their various activities see generally Lee et al., *supra* note 46.

[52] *See infra* text accompanying notes 59 *passim*.

The credit card example was not chosen arbitrarily. In fact, concerns about the security of payments or credit card information are among those most frequently expressed by consumers.[53] This example clarifies that security concerns, in general, are actually concerns about anticipated fraud at a later stage. Shortly before Christmas 1999, in a case that draw extensive media attention,[54] a hacker, "Maxus", claimed that he got access to about 300.000 credit card numbers from customers of online music retailer CD Universe.[55] In fact, he made as many as 25.000 numbers available on a web page after the company refused to pay $100.000. The attempted extortion[56] tried to take advantage of the fear of a subsequent fraudulent use of these numbers. It actually was confirmed that some of the numbers have been used for fraudulent online purchases and the hacker alleged that he had already sold 10.000 of them before the website was eventually shut down.[57] Thus, the security concerns, at least with regard to online

---

[53] *See, e.g.*, OECD, THE IMPACT OF ELECTRONIC COMMERCE, *supra* note 2, at 42 (security of payments); DIGITAL ECONOMY I, *supra* note 4, at 45 (security of credit card information); DIGITAL ECONOMY II, *supra* note 4, at 7 (security of credit card purchases). From a legal point of view, however, this concern, if expressed by *consumers* (i.e. cardholders) is hardly rational, *see infra* note 77.

[54] *See, e.g.*, Will Knight, *Every e-commerce site's nightmare as hacker gets nasty with credit card details*, ZDNet UK (Jan. 12, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12576.html>; Mike Brunker, *Data thief threatens to strike again*, ZDNet UK (Jan. 12, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12574.html>; ZDNet, *Like stealing credit cards from babies*, ZDNet UK (Jan. 13, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12608.html>. *See also* Bob Sullivan, *How to steal 2,500 credit cards*, ZDNet UK (Jan. 17, 2000) <http://www.zdnet.co.uk/news/2000/2/ns-12672.html> (

[55] *See* <http://www.cduniverse.com>.

[56] *See generally*, Tom Steinert-Threlkeld, *It's a new era—of economic blackmail*, ZDNet News (Feb. 9, 2000) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2435665,00.html> (referring to an attack in early Feb. 2000 that took down some of the biggest e-commerce sites, including Yahoo, E*Trade, Buy.com, ZDNet, for several hours as setting the stage for a new type of economic blackmail).

[57] *See also* Randy Gainer, *Allocating the Risk of Loss for Bank Card Fraud on the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 39, 42-44 (1996) (giving similar examples of posting, trading

payment mechanisms, are ultimately concerns about fraud. Note that the victims in these cases[58] will typically be the merchants, not the consumers. The legal situation both in the U.S. and in Europe is straightforward in this respect and clearly suggests that it is the merchants that should be worried about the security of online payment systems because in general *they* will have to bear the risk of loss in these cases.

In the U.S. the use of credit cards is mainly regulated by the Truth-in-Lending Act (TILA)[59] and the Federal Reserve Board's implementing Regulation Z.[60] In the event of an unauthorized use of the credit card (in the online context basically the use of the card data by a third party) the liability of the cardholder is generally limited to a flat $50.[61] One condition for imposing liability on the cardholder at all, however, is that the card issuer has provided a means to identify the cardholder, such as a signature, photograph, or fingerprint on the card.[62] In transactions that do not physically involve the card, such as mail order/telephone order and online transactions, this condition is not met, "[s]ince the issuer has not provided a

---

and selling credit card numbers online that have been stolen while transmitted over the network or from merchants that have neglected server security).

[58] As in the majority of cases if it is true that "the most common types of [fraudulent] activity [are] the use stolen credit cards, false identities and card generators", *see* Leung, *supra* note 21.

[59] Title I of the CONSUMER CREDIT PROTECTION ACT (CCPA) of 1968, 15 U.S.C §§ 1601-1667f. *See generally* RALPH C. CLONTZ, JR., TRUTH-IN-LENDING MANUAL (Update No. 3, 1997).

[60] 12 C.F.R part 226 (1999).

[61] *See id.* § 226.12(b).

[62] *See id.* § 226.12(b)(2)(iii) and Official Staff Interpretations, 12 CFR 226, Supp. I § 12(b)(2)(iii), at 1. (1999).

means to identify the user *under these circumstances*, ....".[63] Therefore, in the event of an unauthorized use of her credit card data in Internet transactions, a cardholder is not liable at all—not even for $50.[64]. Merchants and card issuers are seldom as clear in this respect as Sean Healy, a spokesman for VISA USA, who, referring to the CD Universe case,[65] was cited having said that in most cases there will be "no consumer liability".[66] And while the consumer is basically out of it, the contractual agreements between card issuer and merchant typically shift the risk of an unauthorized use that occurs without the physical presentation of the card and absent a sales slip signed by the card user to the merchant by allowing the card issuer to charge the transaction back to him.[67]

European law leads to the same result. Art. 8 of the European Distance Contracts Directive[68] deals with payment by card in such contracts. It obligates Member States to give consumers the right (that in fact already exists in most of the Member States)[69] "to request cancellation of a payment where fraudulent use

---

[63] *See* Official Staff Interpretations, *supra* note 62, § 12(b)(2)(iii), at 3. (emphasis added). *See also* Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. 675, 687 (1999).

[64] Thus, with regard to online transactions Gainer, *supra* note 57, at 45 (1996) is incorrect when he states that "[w]hile the statute allows card issuers to impose liability up to fifty dollars, this is rarely attempted by lenders; ...." Because of Reg. Z, *supra* note 60, § 226.12(b)(2)(iii), which Gainer does not mention, the issuer could not even impose that liability. Froomkin, *supra* note 3, at 71 n.70 is similarly unclear on that point.

[65] *See supra* note 55 and accompanying text.

[66] *See* Brunker, *supra* note 54.

[67] *See* Kaufman Winn, *supra* note 63, at 687; LARY LAWRENCE, AN INTRODUCTION TO PAYMENT SYSTEMS 515-16 (1997).

[68] *See supra* note 24.

[69] *See* Bundesministerium der Justiz, Referat I B 2, *Referentenentwurf Fernabsatzgesetz* 44 *passim* [*Draft of a German Distance Contracts Act*], Doc. 3420/12-4 (May 31, 1999)

has been made of his payment card in connection with distance contracts covered by this Directive" and "in the event of fraudulent use, to be recredited with the sums paid or have them returned." Thus, in the event of an unauthorized use of the credit card data the card issuer can only impose any liability on the cardholder when the latter acted negligently (e.g. when she left her card somewhere and it is stolen and then misused).[70] However, the transmission of credit card data over the Internet, even over insecure channels, is not regarded as constituting a negligent act by the cardholder.[71] Consequently, as in the U.S., the European cardholder is generally[72] not liable for an unauthorized use of her card data on the Internet. And as in the U.S., the contractual agreements between card issuer and merchant ultimately shift the risk to the latter.[73]

It becomes apparent, that the fact that security attacks of this kind—particularly worries about the security of credit card data—rank among *consumers'* most frequently expressed concerns is mostly[74] due to a common misconception of the

---

<http://www.bmj.bund.de/download/fernag.pdf> [hereinafter BMJ, *Draft Distance Contracts Act*] (citing Rufus Pichler, *Kreditkartenzahlung im Internet*, 1998 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 3234).

[70] Although there is—in these cases of negligent conduct by the cardholder—no legal requirement to limit the cardholders liability (unlike under U.S. law, *see supra* note 61), all card issuers follow a recommendation by the European Commission (*see* Commission Recommendation of 17 November 1988 concerning payment systems, and in particular the relationship between cardholder and card issuer (88/590/EEC), 1988 O.J. (L 317) 55, Annex 8.3, available online at <http://www.europa.eu.int/eur-lex/en/lif/dat/1988/en_388X0590.html>) and limit it to a flat $50 as well. *See* RUFUS PICHLER, RECHTSNATUR, RECHTSBEZIEHUNGEN UND ZIVILRECHTLICHE HAFTUNG BEIM ELEKTRONISCHEN ZAHLUNGSVERKEHR IM INTERNET 74 (1998).

[71] *See* Pichler, *supra* note 69, at 3236 and the sources cited therein.

[72] This can change with the use of secure payment systems such as SET, *see infra* note 85.

[73] *See* Pichler, *supra* note 69, at 3237.

[74] *See infra* note 77.

legal risk allocation in cases of unauthorized use of credit card data.[75] The fact that these worries nevertheless seem to be such an important inhibitor of consumer confidence is probably the result of widespread confusion and a lack of education in regard to the "real" risks. A report by Jupiter Communications finds that great media attention fuels consumer fears and that online businesses must better educate consumers.[76] But when going on that "[c]onsumers have confused the concepts of privacy and security; they identify security of credit card information, which is their primary concern, as a privacy issue", even that report misses the issue in which education seems to be needed most—i. e. that, from the consumer's point of view, the concerns about the security of credit card information are irrationally exaggerated.[77]

---

[75] *See also* Gainer, *supra* note 57, at 48 (concluding that "[c]onsumers should not be concerned about potential theft of their bank card data, because federal statutes generally prevent the consumer from incurring liability for any significant misuse of the card data."); Kaufman Winn, *supra* note 63, at 687 (finding that the high level of consumer protection regarding credit card transactions "minimize the transaction risks assumed by consumers in Internet transactions by shifting the risks back onto the merchant, the merchant's bank or the card issuer."); Froomkin, *supra* note 3, at 76 ("the risk may be smaller than commonly believed").

[76] *See* Jupiter Communications, Press Release, *64 Percent of Online Consumers are Unlikely to Trust a Web Site* (Aug. 17, 1999) <http://www.jup.com/company/pressrelease.jsp?doc=pr990817>. *See also* Jane Wakefield, *Media blamed for consumer online fears*, ZDNet UK (Aug. 18, 1999) <http://www.zdnet.co.uk/news/1999/32/ns-9370.html> (referring to the aforementioned report); Jane Wakefield, *Online fraud warning to all e-commerce users*, ZDNet UK (Feb. 1, 2000) <http://www.zdnet.co.uk/news/2000/4/ns-13032.html> (citing the director of a company that tests networks who warned consumers using the Net for e-commerce: "Be afraid, be very afraid.").

[77] It is true, however, that consumers might face considerable inconveniences. They will have to check their balance statements for unauthorized charges regularly, they might need to invest time to initiate being recredited with the amount charged, they might find it embarrassing to face and contest charges for allegedly using adult entertainment services and so on. Thus, their concerns are certainly not completely irrational. For an example of one concern s*ee The growing threat of internet fraud*, BBC News (Nov. 19, 1999) <http://news.bbc.co.uk/hi/english/business/your_money/newsid_526000/526709.stm> ("Credit-card numbers obtained by theft of from anarchist websites on the Internet are used to access pornographic net pages, and innocent people are charged.").

The merchants, however, who one would expect to really be concerned because they have to bear the loss of online credit card fraud, do not appear to be too worried about security.[78] And there might be good reasons why they—despite all the fuzz—in fact need not be (and even better reasons, why *we* need not worry too much about online merchants becoming victims of credit card fraud either). First, the degree of credit card fraud actually does not seem to be so high after all. Although it is alleged that half of all credit-card disputes concern Internet transactions,[79] "credit card fraud [in general] is at a historical low point (between 7 and 8 cents per $100)",[80] according to Spencer Nilson, whose Nilson Report[81] has been the leading publication on consumer payment systems worldwide for thirty years. It appears that merchants can afford to accept the costs of fraud with regard to increasing returns from a much larger volume of regular transactions.[82] Second, it is in the merchant's own hand to increase the security.[83] And indeed there are various systems that aim to make electronic transactions and online payments more secure—*for merchants*. The widespread use of certified digital

---

[78] *See* Sullivan, *supra* note 54, for an account of how surprisingly shoddy security of some e-commerce sites facilitates the theft of credit card data.

[79] According to information by VISA International, *see Fraud continues to deter e-shoppers*, IT-Analysis.com (Nov. 22, 1999) <http://www.it-analysis.com/99-11-22-2.html>; *The growing threat of internet fraud, supra* note 77.

[80] *See* Brunker, *supra* note 54 (citing Nilson).

[81] *See* <http://www.nilsonreport.com>.

[82] *See* Kaufman Winn, *supra* note 63, at 688.

[83] And from an economic point of view one would expect them to do so as long as the costs of enhancing security are lower than the costs of fraud. To this background there will always be some fraud which to prevent would be inefficient. *See also* Brunker, *supra* note 54 (citing Nilson making a similar point).

signatures[84] and their implementation in secure electronic payment systems such as SET[85] would allow merchants to significantly reduce the risk of consumer fraud.[86] Digital signatures are based on public key encryption.[87] This means a party possesses a unique pair of keys. One is the private key that is secret, under the party's sole control (its use is normally protected by a password known only to that party), and secure (meaning the key can in practice not be forged). The other is a public key that can be freely distributed and is often stored in publicly accessible databases. To make sure to whom a certain public key belongs, a certification authority (CA) is involved.[88] The CA verifies the identity of the user of a key pair and attaches a certificate (that again cannot be forged) with information on the holder of the corresponding private key to the public key.

---

[84] For a recent and comprehensive overview on the technology of digital signatures and the related legal issues see Symposium, *Digital Signature and Electronic Document Verification*, 17 J. MARSHALL J. COMPUTER & INFO. L. 721 (1999).

[85] For a description of the system see SET Secure Electronic Transactions LLC, *What is SET* (visited Aug. 17, 00) <http://www.setco.org/set.html>; VISA, *Internet Shopping: SET* (visited Aug. 17, 00) <http://www.visa.com/nt/ecomm/security/set.html>; MasterCard, *Shop Online: SET* (visited Aug. 17, 00) <http://www.mastercard.com/shoponline/set>. For a legal perspective see Pichler, *supra* note 69, at 3237 *passim*; Kaufman Winn, *supra* note 63, at 689-691.

[86] It has also been argued that it would allow consumers to reduce merchant fraud as well (*see* Kaufman Winn, *supra* note 63, at 691 ("SET was marketed as a solution to the problem of consumer fraud through false claims of unauthorized use of a card as well as to the problem of merchant fraud."). Although it is true that certified digital signatures would tell the consumer with whom she is dealing, her more important problem would remain unsolved: The consumer would still not have a means to effectively and efficiently enforce her rights (e.g. her claim for a refund of the amount paid) against the merchant. For a detailed discussion of this problem see *infra* II.C.1).

[87] I will just very briefly sketch the functionality of digital signatures here. For a more detailed description see, for example, David L. Gripman, *Electronic Document Verification: A Primer on the Technology Behind Digital Signatures*, 17 J. MARSHALL J. COMPUTER & INFO. L. 769 (1999). *See also* Rufus Pichler, *Richtlinienvorschlag zu elektronischen Signaturen*, 1998 EUROPEAN LAW REPORTER 523, 524. For an easy-to-understand explanation of public key encryption and digital signatures see also STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST 1-2 (1998); Froomkin, *supra* note 3, at 51-67.

[88] *See generally* Froomkin, *supra* note 3, at 55-67 (explaining the role and various functions of CA's).

Although the keys belong together and the public key is needed and used to verify a message "signed" with the private key, it is not possible to derive the private key from the public key. A message is signed[89] with the signatory's private key. The recipient then uses the signatory's public key (which is sent with the message or retrieved from a database and includes the certificate) to verify the signature.[90]

To clarify things, note the key characteristics of digital signatures as they are listed in the recent EU Directive on Electronic Signatures:[91] It is (a) *uniquely linked* to the signatory, (b) capable of identifying the signatory, (c) created using means that the signatory can maintain under his sole control, and (d) linked to the data to which it relates that any subsequent change of the date is detectable. From the perspective of the recipient the consequences are the following: She knows (a) that the message she received can come from only one person (i.e. the possessor of the private key), since the key is unique, (b) who the signatory is, (c) that no one other than the signatory has access to the key without the signatory's consent or negligence, and (d) that the signatory has actually sent

---

[89] Signing means that a program creates a hash or message digest of the message, which uniquely identifies this message and is, if created anew, always the same unless the message has been altered. This hash is encrypted with the signatory's private key and then sent with the message.

[90] In fact she uses the public key to decipher the hash and compare it to the hash her program created of the message that has been signed. If the two functions are the same, she knows that the message she received has not been altered.

[91] *See* Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000 O.J. (L 13) 12, art. 2(2). *See generally* Rufus Pichler, *Signaturrichtlinie*, 2000 EUROPEAN LAW REPORTER 75 (giving an overview on and analyzing the Directive).

*exactly the message received* (i.e. that there has been no forgery in the course of the transmission).

Thus, when integrated into payment systems, digital signatures can effectively take care of merchants' security concerns and practically eliminate consumer fraud. Consequently one need not worry too much about merchants becoming victims of consumer fraud, because if the problem would really get out of hand, one can expect to quickly see a more widespread implementation of systems like SET.[92]

What raises a little more concern, however, is the opposite scenario: consumers becoming the victims of *merchant fraud*.

### *2) Merchant Fraud and Consumer Redress*

As a matter of fact, it typically is the consumer who bears the risk of prior performance that is inherent to remote transactions. In general, merchants will require some kind of *advance payment* before sending goods to a consumer or granting her access to information or other services.[93] In most online transactions

---

[92] To date a broad implementation cannot be observed, however. This is partly due to the fact that SET not only very secure, but also "complex and cumbersome" (*see* Kaufman Winn, *supra* note 63, at 690), and probably mostly to the fact that in regard to the relation between returns and the total volume of chargebacks merchants have not seen the economic benefits, let alone necessity, to switch to a more secure system. *See also id.* at 697 (describing why so far everybody with the status quo relying on SSL which does not use digital signatures and basically only provides for security of the data during the process of transmission; it does not, however, prevent consumer fraud).

[93] *See, e.g.*, ACCC, *Enforcement Challenge, supra* note 28, at 11 ("payment for goods and services in the global marketplace is often made in advance"); Frank Diedrich, *Internationales Einheitsrecht—Internationalisierung der Rechtswissenschaft?, in* JAHRBUCH JUNGER ZIVILRECHTSWISSENSCHAFTLER 1998: VERNETZTE WELT—GLOBALES RECHT 45, 65 (Martin Immenhauser & Jürg Wichtermann eds., 1999) (emphasizing the practice of advance payment).

that "payment" will consist of an authorization to charge the consumer's credit card,[94] although there exist a variety of alternative electronic payment systems.[95] Almost all non-cash forms of payment aim at creating a high degree of finality[96] by making it hard if not impossible for the payer to simply reverse the payment once she authorized it.[97] A higher degree of finality reduces the merchants' risk[98] and at the same time assigns the risk of prior performance to the consumer, who will eventually have to take action to make the merchant repay the amount if she

---

*See also* Consumers International, Consumers@shopping: *An international comparative study of electronic commerce* 35 (Sept. 1999) <http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf> (finding that "[i]n 71% of cases researchers had to pay for goods before they arrived, ....").

[94] Credit cards are by far the prevailing payment method in business-to-consumer e-commerce. *See* Kaufman Winn, *supra* note 63, at 687 (speaking of the "current dominance of credit cards as the payment device of choice for retail Internet services."); John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAW. 403 (1998) ("by far the dominant form of payment for Internet transactions.").

[95] *See generally* PICHLER, *supra* note 70; Pichler, *supra* note 69; Muller, *supra* note 94; Robert F. Stankey, *Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers*, 6 COMMLAW CONSPECTUS 11 (1998); Gainer, *supra* note 57; Kaufman Winn, *supra* note 63; Dan L. Nicewander, *Electronic Banking—Smart Cards, Cyberspace and the Internet*, 50 CONSUMER FIN. L.Q. REP. 22 (1996) (all discussing new electronic payments systems for the Internet and related legal issues).

[96] Cash has an absolute finality. Once it is handed over to the merchant, the payment cannot (legally) be reversed by an act of the payer alone. Merchants accepting alternative forms of non-cash payment (like checks, electronic funds transfer, debit cards, credit cards etc.) have always been longing for a comparable level of finality, since they did not want to assume the risk of the payer reversing the payment afterwards. The specific degree of finality and the point in time at that a payment becomes final, however, vary from payment system to payment system and from country to country. In Germany, for example, most non-cash forms of payment have a high degree of finality, mostly due to guarantees of payment by banks or other payment providers (examples include the guaranteed "euro-cheque", or credit cards under certain conditions, and new Internet payment systems like CyberCoin or Digicash). *See* PICHLER, *supra* note 70, at 19 n.90 and accompanying text. In the U.S. the degree of finality, at least in regard to checks and credit cards, is lower. *See, e.g.*, Kaufman Winn, *supra* note 63, at 683, 686 (pointing to the low degree of finality of checks and credit cards, respectively).

[97] *See generally* Kaufman Winn, *supra* note 63, at 679 (describing finality of payments and its significance for payer and payee).

[98] *See also* Froomkin, *supra* note 3, at 69 (pointing out that merchants generally desire nonrepudiation of a consumer's order and assurance that payment will be made, which can be achieved "by having payment before sale, at time of sale, or by provision of a payment guarantee").

feels it is not entitled to keep it. Thus, finality of payment in effect allocates the burden of having to take (legal) action in the event of a dispute. It is not the merchant who needs to bring an action against the consumer to get the money, but it is the consumer who needs to bring an action if, for some reason, she wants her money back. Finality of payment or the consumer's ability to reverse payments and thus shift the burden of taking action back to the merchant are crucial issues in the context of effective enforcement of consumer rights and enhancement of consumer confidence.[99]

Assume for now[100] that the risk of prior performance, which is equivalent to the burden of taking action to retrieve the amount paid, is typically born by the consumer—due to the merchants' insistence on advance payment in one form or the other.[101]

To this background there are a number of scenarios, an online shopper could—some suggest should[102]—be worried about.[103] To begin with, consumers face a

---

[99] *See infra* note **Fehler! Textmarke nicht definiert.** and accompanying text.

[100] This assumption is definitely realistic with regard to European consumers. *See supra* note 96.

[101] *See supra* notes 96-98 (explaining methods of advance payment or charge or equivalent payment guarantees).

[102] *See* Wakefield, *supra* note 76, and the citation restated there: "Be afraid, be very afraid."

[103] *See also* Rothchild, *supra* note 31, at 903-911 (listing varieties of online deceptive marketing practices, distinguishing fraudulent and misleading online conduct and citing DANIEL J. BARRETT, BANDITS ON THE INFORMATION SUPERHIGHWAY 47-122 (1996) for a discussion of the varieties of Internet-based fraud); Hebe R. Smythe, *Fighting Telemarketing Scams*, 17 HASTINGS COMM. & ENT. L.J. 347, 350 *passim* (1994) (describing various telemarketing scams).

variety of scams and fraudulent "merchants" on the net.[104] Rothchild[105] gives numerous examples for pyramid schemes, chain letters, bogus business opportunities, credit repair schemes, "miracle" health or diet products, investment and securities scams, and fraudulent gambling sites.[106] On legal e-mail lists[107] an increasing number of postings report cases in which adult entertainment sites asked users for their credit card information "for age verification only" and subsequently charged their account alleging that the user agreed to a subscription.[108] Scams like these[109] presumably also profit from the fact that victims are too embarrassed to contest the charges.[110] They are obviously also responsible for the following warning, which could be found on Citibank's

---

[104] It is interesting to note that, according to a survey of 100 retailers cited by Leung, *supra* note 21, "41 per cent of respondents did not realise that merchants themselves were also responsible for online fraud, however."

[105] *See supra* note 103.

[106] For more examples and a short description of numerous cases see Federal Trade Commission, Report, *The FTC's First Five Years Protecting Consumers Online* 8 *passim* (Dec. 1999) <http://www.ftc.gov/os/1999/9912/fiveyearreport.pdf> [hereinafter FTC, *First Five Years*] (listing hijacking, web cramming, pyramid schemes, credit scams, auctions, business and investment opportunity scams, and health claims).

[107] *See, e.g.*, Bernd Goecke, *Re: Kreditkarten im Internet* (Feb. 18, 2000), posted to netlaw-l@listserv.gmd.de, available online in the list's archive at <http://www.listserv.gmd.de/htbin/wa.exe?A2=ind0002&L=netlaw-l&F=&S=&P=23268> (reporting a case the Goecke, a German lawyer, represented).

[108] *See also* FTC v. J.K. Publications, Inc., No. CV-990004 ABC (AJWx) (C.D. Cal. filed Jan. 5, 1999) (monthly charges of $19.95 for "adult Internet services" that consumers allegedly had never ordered).

[109] The practice of billing for unauthorized services (in addition to the cases described above this includes, for example, billing consumers after promising a "free trial period", *see* FTC v. U.S. Republic Communications, Inc., No. H-99-3657 (S.D. Texas filed Oct. 21, 1999)) is called "cramming", *see, e.g.,* FTC, *First Five Years, supra* note 106, at 9. *See also* FTC v. Shared Network Services, LLC, No. CIV. S-99-1087 WBS JFM (E.D. Cal. filed June 2, 1999); FTC v. WebViper, LLC, 99-T-589-N (M.D. Ala. filed June 9, 1999); FTC v. Wazzu Corporation, SACV-99-762-AHS (C.D. Cal. filed June 7, 1999) (in all cases defendants allegedly charged customers despite offering a "free 30-day-trial").

[110] *See also supra* note 77.

German VISA billing statements: "A tip for Internet users: Your Citibank Visa Card can also be used very well on the Internet, since it is accepted by a large number of merchants. We recommend, however, not to transmit your card number in regard to free offers. These may lead to subscriptions, that will result in charges to your Visa card account."[111]

While it might be argued that the examples of online scams and fraudulent merchant behavior given above are in some way special since their mere content should make users suspicious, there are other types of fraud that can occur in any "everyday" transaction.

The clearest of these cases certainly is that in which the goods or services the consumer paid for are never delivered.[112] Since setting up an online "shop"—which potentially reaches a global market—requires next to no start-up investment and incurs very low operating costs,[113] the Internet appears to provide an almost perfect environment for scams of this kind.[114] "Merchants" do

---

[111] Citcorp Card Operations GmbH Billing Statement to the author (Oct. 22, 1999) (on file with author) (translation by author).

[112] *See* Rothchild, *supra* note 31, at 906 (citing a number of FTC decisions); ACCC, *Enforcement Challenge*, at 11.

[113] *See* Carey Heckman, *Gateways to the Gobal Market: Consumers and Electronic Commerce* at 1.2 (visited Aug. 17, 00) <http://www-techlaw.stanford.edu/pages/OECDBack.html> ("All enterprises, including the small and medium-sized, can reach customers throughout the world instantly and comparatively inexpensively.").

[114] *See* ACCC, *Enforcement Challenge, supra* note 28, at 15 (listing a number of features that make the Internet "an attractive means of operation for unethical traders", including easy entry, access to consumers worldwide promising high turnovers, anonymity and the ease of escaping detection, the transitory nature of the business which allows to close up operations and set up new schemes in different countries quite easily); FTC, *First Five Years, supra* note 106, at 3 ("It [the online marketplace] is just as attractive to the fraudster as it is to the legitimate business. It is cheap and easy to enter, and it enables a worldwide reach. It offers anonymity and easy exit, often before authorities have the chance to detect wrongdoing."); FTC, *New Tools of the Trade*,

not need to rent a physical store; they do not need to display any items and must not be personally present. They can simply design a website offering various products or services that they do not actually have or can provide and, of course, never intend to deliver. Before people realize that they became victims of a scam, the "shop" (i.e. the website) might already have closed down and "reopened" under a different name and design, targeting different users.[115] The identity and the actual physical location of the people behind it will generally be very hard to track.

Quite similar to opening a website and selling products or services with the intent not to perform after the consumer's payment has been received is "spoofing".[116] Here the fraudster doesn't set up her own online shop, but assumes the identity of a well known company and accepts orders and payments for products or services actually sold by that company.[117] Neither orders nor payments, of course, ever reach that company—just as the services or products purchased never reach the consumer. Other types of merchant fraud include misleading or

---

*supra* note 50, at 3 ("Con artists also are online, hoping to take advantage of low startup costs; the possibility of 'real-time' immediate payments; a nearly infinite number of places to 'hide' from law enforcement; unparalleled ability to mimic legitimate business; and instant access to a global customer base. Today's fraud peddlers can confuse consumers more easily through web sites that are as sophisticated and appealing as those of many legitimate businesses.").

[115] For similar scam schemes in the telemarketing world see Smythe, *supra* note 103, at 351 ("Before the victims discover the fraud, the yak unplugs the telephones and moves to another location to begin a new scam."). Moving to another "location" is obviously much easier online.

[116] *See, e.g.*, Rothchild, *supra* note 31, at 908 (describing spoofing).

[117] *See also* FTC, *New Tools of the Trade*, at 16 (describing cases of deceptive URL's, including http://www.internic.com, the site of an Australian company that designed a look-alike site to Network Solution's site, whose URL was http://www.internic.org, and, posing as Network Solutions, offered to register domains for a fee of $250 while Network Solution's fee was only $100).

deceptive information—for example charging a higher price than has been stated on the website[118]—and misrepresentations regarding the product offered.[119] Finally it is possible that merchants do not honor rights of return[120] that they have previously granted themselves or that are granted by law.[121]

And even when a merchant is not actually acting fraudulently, it will have to be conceded that "from time to time things go wrong in cross-border transactions."[122] Goods might arrive, but they may be defective or otherwise unsatisfactory, and they might—especially during the holiday season[123]—arrive

---

[118] The story of David J. Loundy's attempt to buy a rare CD of the group Level 42 from a British Web site provides a fun-to-read example for this (although the merchant in that case presumably did not actually have a fraudulent intent); *see* Carl S. Kaplan, *On the Web, It's Buyer Beware. But Where?*, N.Y. TIMES, CYBER LAW JOURNAL (March 26, 1999) <http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/26law.html>.

[119] For a variety of examples for these and other practices see ACCC, *Enforcement Challenge, supra* note 28, 15-19.

[120] *See* ACCC, *Enforcement Challenge, supra* note 28, at 11.

[121] Art. 6(1) of the Distance Contracts Directive, *supra* note 24, for example, grants consumers the right to withdraw from any distance contract within a period of (at least) seven working days without penalty and without giving any reason. The exercise of this right leads to an obligation of the supplier to reimburse the sums paid by the consumer, *see id.* art. 6(2).

[122] *See* ACCC, *Enforcement Challenge, supra* note 28, at xi.

[123] *See* Connie Guglielmo, *Consumer reluctant to rely on Net*, ZDNet UK (Dec. 13, 1999) <http://www.zdnet.co.uk/news/1999/49/ns-12127.html> (referring to a study by Jupiter Communications finding that fears of orders being shipped late or that items will be out of stock are two of the main reasons why most consumers will continue to do their holiday shopping offline). These fears are obviously not ungrounded, *see* Saul Hansell, *Toys 'R' Us Falls Behind on Shipping*, N.Y. TIMES, Dec. 23, 1999, at <http://www.nytimes.com/library/tech/99/12/biztech/articles/23toy.html>. *See also* Louise Kehoe, *A Valentine's Day fiasco,* FT.com (Feb. 20, 2000) <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT4KVRU4X4C> (describing Valentine's day delivery problems of online greeting card providers and florists).

late.[124] Again, the risk of prior performance in all of these cases lies with the consumer, who will have to take action to get his money back.

Unfortunately, these examples of fraudulent merchant behavior or of other problems in the transaction to the consumer's disadvantage are by no means purely theoretical. They do happen in practice, and they do happen to an extent that makes the danger of an erosion of consumer confidence in the electronic marketplace appear more than likely. A list of the Federal Trade Commission's Enforcement Actions Involving the Internet and Online Services as of Dec. 15, 1999 shows 107 cases in which the Commission took action against fraudulent merchant conduct.[125] This list, of course, covers only a fraction of fraudulent online conduct, as it is limited to enforcement actions of *one* enforcement agency in *one* country and naturally does not include the presumably much larger number of cases that have not been discovered (before the sites disappeared) or in which enforcement actions have not been or could not be taken for various reasons. A study by Consumers International, in which researchers from 11 countries placed a total of 151 orders from sites in 17 countries between November 1998 and February 1999[126] found that 9% of the goods ordered never

---

[124] *See* ACCC, *Enforcement Challenge, supra* note 28, at 11. *See also* Forrester Research, Inc., Press Release, *eCommerce Could Be Hindered By Order Fulfillment Chaos* (Aug. 26, 1999) <http://www.forrester.com/ER/Press/Release/0,1769,160,FF.html>.

[125] *See* Federal Trade Commission, *Commission Enforcement Actions Involving the Internet and Online Services* (Dec. 15, 1999) <http://www.ftc.gov/opa/1999/9912/case121599.pdf> [hereinafter FTC, *Cases*].

[126] *See* Consumers International, *supra* note 93, at 19-22 (describing the methodology of the study).

arrived;[127] that in 20% of cases the amount actually charged was higher than the purchaser expected;[128] and that, where a return was possible,[129] there were problems in obtaining a refund of the purchase price in 21% of purchases.[130] According to another survey,[131] which was supported by the European Commission, an even higher percentage of goods—18.1%—never arrived, and of the goods that did arrive, 7% were either damaged or late;[132] 27.8% of customers who returned goods did *not* receive a refund;[133] and in 6% of the cases in which payment was made by credit card, the account was charged but the goods were never delivered.[134] Moreover, with regard to telemarketing fraud it has been found that it costs consumers an estimated fifteen billion to forty billion dollars each year.[135] And given the fact that the main factors that made (and make) telemarketing fraud "a lucrative and profitable business for scam artists"[136] are believed to be the anonymity of the telephone and the ease of

---

[127] *See id* at 37. In one of these eleven cases (app. 1%) the consumer was charged nevertheless.

[128] *See id* at 35.

[129] In a number of cases the time limits for returning goods had elapsed before receipt of the item, and in others the cost of returning was higher then the price of the item.

[130] *See id* at 39.

[131] *See* Stiftung Warentest, *Electronic commerce in Europe* (Sept. 1999) <http://www.europa.eu.int/comm/dg24/library/surveys/sur11_en.pdf>. The methodology is described *id.* at 9.

[132] *See id.* at 39-40.

[133] *See id.* at 37. In over 90% of these cases the merchant gave no reason for the non-refund or failed to reply, *see id.* at 36.

[134] *See id.* at 38.

[135] *See* Smythe, *supra* note 103, at 350 and sources cited therein.

[136] *Id.*

escaping detection,[137] one can only expect the problem to be aggravated in the online environment.

These examples and findings suggest that there actually is sufficient reason for consumers to not feel completely comfortable with shopping online. To this background the commonly expressed concerns about a lack of consumer confidence or consumer trust, which were referred to above,[138] seem plausible.[139] But what do the terms "consumer confidence" and "trust" actually mean, and what are they based upon?

## B. What is "Consumer Confidence"?

Electronic commerce[140] ultimately is about completing transactions between merchants and consumers. Putting it very simple, and leaving non-transactional issues such as privacy[141] aside, one can assume that a consumer enters into a transaction (in our case an exchange of the consumer's money for the

---

[137] *Id.* (citing *Telemarketintg Fraud: Hearing Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, and Transp.*, 102d Cong., 2d Sess. 4 (1992)).

[138] *See supra* text and notes following note 13. According to another survey cited by Leung, *supra* note 21, "[t]he majority of retailers ... viewed lack of consumer confidence as their number one concern."

[139] *Cf.* Smythe, *supra* note 103, at 368 (asserting, with regard to telemarketing scams, that "[p]ublicity about fraudulent telemarketers makes consumers generally more suspicious and reluctant to purchase goods by telephone, and telemarketers may have difficulty regaining the confidence of consumers who have been defrauded by unscrupulous scam artists" and citing *Hearing Before the Subcomm. on Transp. and Hazardous Materials of the House Comm. on Energy and Commerce*, 103d Cong., 1st Sess. 45 (1993) and H.R. Rep. No. 103-20, 103d Cong., 1st Sess. 2 (1993)).

[140] As stated above, *supra* I, I will concentrate on business-to-consumer electronic commerce in this paper.

[141] *See supra* notes 47-49.

merchant's goods or services) only if she believes that "things go right"[142] or that "things can be fixed if they go wrong".[143] To be a little more specific in regard to online transactions one can say that a rational consumer enters into a transaction if she believes that she will actually get the goods (in the condition agreed upon) or services she is about to pay for, or if she believes that something can be done, that some remedy or some kind of redress is available, to prevent her from incurring a permanent loss if she doesn't get what she paid for.[144]

To be sure, not every consumer acts rational all of the time. Some might not care and take a chance and just "try it out", especially when the amount involved is comparably small. But it seems fairly straightforward that this cannot be assumed in the majority of cases, and that even those who do not care once or twice will probably do so at some point (or they loose interest in trying it out altogether). Moreover, the underlying expectation when taking a chance very often is that things go right. Finally, even those who are generally skeptical about neoclassical economics' rational choice theory concede that it is "correct about

---

[142] *See, e.g.*, OECD, *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce* 2 (Dec. 9, 1999) <http://www.oecd.org/dsti/sti/it/consumer/prod/CPGuidelines_final.pdf> [hereinafter OECD, *Consumer Protection Guidelines*] (explicitly "[r]ecognising that consumer confidence in electronic commerce is enhanced by the continued development of transparent and effective consumer protection mechanisms that limit the presence of fraudulent, misleading or unfair commercial conduct online").

[143] *Cf.* DOUGLASS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE, AND ECONOMIC PERFORMANCE 33 (1990) ("Enforcement poses no problem when it is in the interests of the other party to live up to agreements. But without institutional constraints, self-interested behavior will *foreclose complex exchange*, because of the uncertainty that the other party will find it in his or her interest to live up to the agreement.") (emphasis added).

[144] *See also* Froomkin, *supra* note 3, at 69 (listing "[c]omfort that there is recourse if the seller fails to perform or deliver" among the buyer's desires); WORKING GROUP II, *supra* note 4, at 17

eighty percent of the time."[145] This is more than enough for the general tendencies that are explored in this paper.

Thus, the basic assumption is that consumers will engage in transactions if they believe that they will get what they pay for or that something can be done if they don't. A similar idea is expressed in the passage from the U.S. Government's Global Framework for Electronic Commerce cited above.[146] This section emphasizes that "consumers must have confidence that the goods and services offered are fairly represented, that they will get what they pay for, and that recourse or redress will be available if they do not."

### *1) Trust and Reliance*

These two expectations—expecting to get it, and expecting being able to fix it if one doesn't get it—need to be clearly distinguished. They can both be put under the generic expression "consumer confidence" but it is important to realize that they are two separate elements. They differ in the bases they are grounded on, they differ in the addressees of the consumer's respective expectations, they differ in the way they are affected by the characteristics of online transactions, and they differ in regard to the means that can be employed to enhance them. The following refers to these two expectations, that together form consumer

---

("Consumer confidence also requires that consumers have access to fair and effective redress if they are not satisfied with some aspect of the transaction.").

[145] *See* FRANCIS FUKUYAMA, TRUST 13, 17 (1995).

[146] *See supra* note 15.

confidence,[147] as *trust* and *reliance*: Trust, if the consumer believes things will go alright, reliance if she believes thinks might go wrong but can be cured if they do. The distinction between trust and reliance is rarely clearly made in the literature, although it has important implications. The following sections will explain in some more detail, how the terms trust and reliance are used in this paper.

### a) Trust

As indicated above,[148] the literature on trust is burgeoning.[149] As this quantity suggests, the authors look at trust not only from different points of view (for example from an economical, psychological, or sociological perspective), but also in very different contexts. Three—partly interrelated—prime areas of interest appear to have evolved in the academic discourse on trust.[150] The first and most

---

[147] The terminology as it is used in this paper does not claim apply generally. Others have, for example, clearly distinguished *confidence* and *trust*. *See, e.g.*, Niklas Luhmann, *Familiarity, Confidence, Trust: Problems and Alternatives, in* TRUST(Gambetta ed.), *supra* note 23, at 94, 97 who differentiates between confidence and trust, asserting that the former relates to things that cannot be influenced by an individual or in regard to which she does not consider alternatives, while pertaining to the latter an individual chooses her own actions in preference to others in spite of the possibility of being disappointed). *See also* Roger C. Mayer et al., *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709, 713 (1995) (referring to Luhmann, *id.*).

[148] *See supra* note 22.

[149] *See, e.g.*, FUKUYAMA, *supra* note 145; TRUDY GOVIER, DILEMMAS OF TRUST (1998) [hereinafter GOVIER, DILEMMAS OF TRUST]; TRUDY GOVIER, SOCIAL TRUST AND HUMAN COMMUNITIES (1997) [hereinafter GOVIER, SOCIAL TRUST]; MARTIN HOLLIS, TRUST WITHIN REASON (1998); TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22; TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH (Roderick M. Kramer & Tom R. Tyler eds., 1996) [hereinafter TRUST IN ORGANIZATIONS]; Russell Hardin, *Trust, in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 623 (Peter Newman ed., 1998) [hereinafter THE NEW PALGRAVE]; TRUST (Gambetta ed.), *supra* note 23; BERNHARD BARBER, THE LOGIC AND LIMITS OF TRUST (1983); JOHN O. WHITNEY, THE ECONOMICS OF TRUST: LIBERATING PROFITS AND RESTORING CORPORATE VITALITY (1995); PriceWaterhouseCoopers, *E-Business: A Matter of Trust* (1999) <http://www.e-business.pwcglobal.com/pdf/trust.pdf> [hereinafter PWC, *E-Business*]; Bruce Chapman, *Trust, Economic Rationality, and the Corporate Fiduciary*, 43 U. TORONTO L.J. 547 (1993).

[150] This is, of course, a very broad categorization, which is not meant to imply that these areas are always clearly separable or independent of each other.

general focus of attention, which to some extent forms the underlying basis for the others, is *social trust*. The level of trust in societies or communities as a whole has stood in the center of Fukuyama's,[151] Hollis'[152] and Govier's[153] work. Govier further analyzed trust in personal relationships (friendship, family),[154] while Fukuyama emphasizes the relation between social trust or "sociability" and economic performance. He claims that "a nation's well being, as well as its ability to compete, is conditioned by a single, pervasive cultural characteristic: the level of trust inherent in the society."[155] Thus, Fukuyama bridges the first focus of attention with the second, *trust within organizations*.[156] The argument goes that within a company mutual trust and cooperation between, for example, management and employees rather than tight controls, hierarchical power, or surveillance enhance efficiency and productivity.[157] The third focus of the literary discussion is *trust in exchange relationships*.[158] It is this aspect of trust—more

---

[151] *See* FUKUYAMA, *supra* note 145.

[152] *See* HOLLIS, *supra* note 149, at 1 (citing and agreeing with John Locke, who "declared trust to be 'the bond of society', the *vinculum societas*, ....") (italics in the original).

[153] *See* GOVIER, SOCIAL TRUST, *supra* note 149.

[154] *See* GOVIER, DILEMMAS OF TRUST, *supra* note 149.

[155] *See* FUKUYAMA, *supra* note 145, at 7.

[156] Or *intraorganizational trust*. *See, e.g.*, Jörg Sydow, *Understanding the Constitution of Interorganizational Trust, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 31 (distinguishing *intra-* and *inter*organizational trust).

[157] *See, e.g., id.* and the sources cited therein; FUKUYAMA, *id.* at 231.

[158] *See generally*, Mari Sako, *Does Trust Improve Business Performance?, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 88 (conceptualizing interorganizational trust into contractual trust, competence trust, or goodwill trust according to its sources); Julia Porter Liebeskind & Amalya Lumerman Oliver, *From Handshake to Contract: Intellectual Property, Trust, and the Social Structure of Academic Research, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 118, 121 (defining "interpersonal trust" as trust that is directly engendered when two actors are involved in an exchange relationship over time); Simon Deakin & Frank Wilkinson, *Contract Law and the Economics of Interorganizational Trust, in* TRUST WITHIN AND BETWEEN

specifically the trust among the partners of a (future) business transaction—that is of interest in the context of this paper. And although most authors to date have concentrated on trust between organizations or *interorganizational trust*,[159] it is no question that similar issues arise in regard to transactions between individuals or between individuals and organizations—in our context between a consumer and a merchant potentially engaging in a business transaction over the Internet. Thus, trust in exchange relationships or *interpersonal* trust[160] appears to be the more appropriate terminology in our context.

As discussed above, there are different types of trust and numerous perspectives and contexts from and in which trust can be analyzed. Thus, it is hardly surprising that one can find almost as many definitions and perceptions of trust as authors that have written on it. Brenkert, for example, identifies the different understandings of trust, which have been used in the literature as "the *Attitudinal, Predictability, and Voluntarist* senses of trust."[161] Rejecting the first two, he favors the Attitudinal sense of trust which basically involves an attitude to act in certain ways in light of the beliefs one has about one's own vulnerability and the other party's restraint to take advantage of that vulnerability.[162] Similarly, according to

---

ORGANIZATIONS, *supra* note 22, at 146; Mayer et al., *supra* note 147, at 711 (speaking of "the relationship between two specific individuals and the reasons why a trustor would trust a trustee" and of *interpersonal trust*).

[159] *See* sources cited *supra* note 158.

[160] *See* authors cited *supra* note 158.

[161] *See, e.g.*, George G. Brenkert, *Trust, Morality, and International Business, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 272, 274-277.

[162] *See id.* at 274.

Govier, "[t]rust is fundamentally an attitude, based on beliefs and feelings and implying expectations and dispositions."[163] For Fukuyama, who focuses on social trust and thus has a much broader approach, "[t]rust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of the other members of that community."[164] As indicated before, there are many other definitions of trust, some more similar to these and some less, some stressing certain factors more and others less.[165]

It is not my focus here, to add another general definition of trust. In fact, given the versatility of approaches to trust, it appears dubious whether one can satisfyingly define trust outside a specific context at all.[166] Therefore I will confine myself to pointing out the characteristics of trust that appear most relevant in regard to business transactions, thus clarifying how trust is understood in the context of this paper. These key characteristics are *uncertainty*, *risk*, and *expectations* with regard to a transaction and the partner to that transaction. To some extent these

---

[163] *See* GOVIER, SOCIAL TRUST, *supra* note 149, at 3. *See also* GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 6 ("Trust is in essence an attitude of positive expectation about other people, a sense that they are basically well intentioned and unlikely to harm us.").

[164] *See* FUKUYAMA, *supra* note 145, at 26.

[165] *See also* Hardy et al., *supra* note 22, at 69 (conceptualizing trust in terms of communication, predictability and goodwill and defining it as a "communicative, sense-making process that bridges disparate groups" and that can be said to exist between partners, "when relations involve a high degree of predictability, on all sides, that the others will not engage in opportunistic behavior."); Christel Lane, *Introduction: Theories and Issues in the Study of Trust, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 1. 4-14 (discussing a number of different views of trust).

[166] *Cf.* Reinhard Bachmann, *Conclusion: Trust—Conceptual Aspects of a Complex Phenomenon, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS, *supra* note 22, at 298, 299-301 (conceding the difficulties to find suitable terms for a social mechanism which is as complex and multidimensional as the concept of trust).

elements can be regarded as a "common denominator" of most otherwise varying definitions of trust.[167]

The first element of a trust relationship is uncertainty as to the other side's future behavior. In this respect I agree with Brenkert in rejecting the Predictability view of trust.[168] If one can actually "predict accurately the behavior of the person trusted",[169] there is no need for trust.[170] In fact, if I knew accurately that the other would not keep her promise, I would do anything *but* trust him. Thus, *knowing* and *trusting* are two different and mutually exclusive states of mind. It is the lack

---

[167] *See also* Lane, *supra* note 165, at 3 (stating that "most concepts of personal trust share three common elements." According to Lane these elements are a degree of interdependence, the presence of risk or uncertainty, and a belief or expectation that the trusting party's vulnerability will not be taken advantage of by the other party); Humphrey, *supra* note 23, at 216-17 (finding that "[t]he many available definitions of trust have two core elements: an agent's acceptance of risk from the actions of others, and the expectation that the 'partner' will not take advantage of the opportunities opened up by the agent's acceptance of risk."); Mayer et al., *supra* note 147, at 712 (defining trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party").

[168] *See* Brenkert, *supra* note 161, at 276. *See also* Virginia Held, *On the Meaning of Trust*, 78 ETHICS 156 (1968) (Held disagrees with Gordon Tullock, *The Prisoner's Dilemma and Mutual Trust*, 77 ETHICS 229 (1967) whom she interprets as follows: "He [Tullock] proceeds to consider the term 'trust' to mean, in effect, being able to *predict accurately* the behavior of the person trusted, ...." Held, *id.* at 157, goes on to argue that "trust seems to have more to do with situations of *uncertainty* than with situations of *certainty*."); Dasgupta, *supra* note 23, at 51 (conceiving of trust as "*correct expectations* about the actions of other people") (emphasis added) (emphasis in original omitted); HOLLIS, *supra* note 149, at 10 ("[T]rust is simply a matter of predictability." Hollis distinguishes two varieties of trust, however, the second being perceived as expecting another person to or predicting that she will "do what is right."); Note, however, that some authors who speak of "predictability" use the term in the sense of "expectation". *See* Hardy et al., *supra* note 165, at 66 (referring to NIKLAS LUHMANN, TRUST AND POWER (1979) who argues "that we make predictions (or have expectations) concerning the behavior of others").

[169] *See* Held, *supra* note 168 (citing Tullock).

[170] *See* Mayer et al., *supra* note 147, at 711 ("The *need* for trust only arises in a risky situation."). *Cf.* Dasgupta, *supra* note 23, at 51 (arguing that trust loses its potency when one can monitor what others have done *before* choosing her own action); LUHMANN, *supra* note 168, at 33 (arguing that the clues employed to form trust do not eliminate, but just reduce the risk, that they do not supply complete information about the likely behavior of the person to be trusted, and that they simply serve as a "springboard for the leap into *uncertainty*") (emphasis added).

of accurate knowledge or predictability that brings about the question of whether I should or should not trust someone to begin with.

Without uncertainty there would also be no *risk*, which is the second, though inseparably related to the first, element of trust in exchange relationships. Not only is trust not needed, when one knows the other party's behavior, i.e. when absent any uncertainty, but, moreover, "[t]rust is only required if a bad outcome [of the other's uncertain behavior] would make you regret your action",[171] i.e. when a risk exists. Risk is, in fact, "one of the few characteristics common to all trust situations."[172] Risk "arises because trusting behaviour exposes the agent to the presumed opportunistic behaviour of her business partner."[173] The trusting party will typically make a *precommitment* of some kind[174] and runs the risk of

---

[171] Luhmann, *supra* note 147, at 98. *See also* LUHMANN, *supra* note 168, at 25 (arguing that trust is involved in those expectations that concern conduct in the light of which one commits one's own actions and which if unrealized lead one to regret one's behavior).

[172] Mayer et al., *supra* note 147, at 712. *See also* Sydow, *supra* note 156, at 35 ("Trust, ..., is always associated with a particular risk on the side of the trusting party.") (also citing et al., *supra*). The fact that the notion of risk is present in almost every definition of trust has already been indicated, *see supra* note 167.

[173] Lane, *supra* note 165, at 3.

[174] *See* LUHMANN, *supra* note 168, at 25. A *pre*commitment in a literary sense is not compelling, however. As Hofstadter's alteration of the original prisoner's dilemma to a trader's dilemma vividly illustrates, simultaneous but secret actions will raise the same issues of trust; *see* DOUGLAS R. HOFSTADTER, METAMAGICAL THEMAS: QUESTING FOR THE ESSENCE OF MIND AND PATTERN 715 (1985): "Assume you possess copious quantities of some item (money, for example), and wish to obtain some amount of another item (perhaps stamps, groceries, diamonds). You arrange a mutually agreeable trade with the only dealer of that item known to you. You are both satisfied with the amounts you will be giving and getting. For some reason, though, your trade must take place in Secret. Each of you agrees to leave a bag at a designated place in the forest, and to pick up the other's bag at the other's designated place. Suppose it is clear to both of you that the two of you will never meet or have further dealings with each other again. Clearly, there is something for each of you to fear: namely, that the other one will leave an empty bag." *See also* Dasgupta, *supra* note 23, at 51 (pointing out that it is the "inability to monitor others' action" that is crucial to the definition of trust and that this inability will in many cases be "be due to the fact that my choice of action temporally precedes those of others", but not in all of them).

suffering a loss, if the other party (the trustee) does not keep her promise or does not live up to her obligation in the exchange. Thus, "[t]rust is a risky business because the people whom we trust can let us down, and we are vulnerable to harm when they do so."[175]

One takes this risk because of one's *expectations*—the most important element of trust. The trusting party expects the trustee *not* to take advantage of or exploit her vulnerability.[176] She believes her, the trustee, not to behave opportunistically and benefit from her, the trustor's, precommitment without keeping her own promise. In other words, trust entails the belief that for some reason[177] the trusted party does not go for a probably greater immediate advantage, i.e. getting something for nothing, but gives something in return, thereby reducing her own advantage but making it a *mutually beneficent* relationship.[178] And again,[179] could the other party's behavior be accurately predicted (instead of just having expectations) there would be no need for trust. Accordingly, Baier defines trust

---

[175] GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 8. *See also* LUHMANN, *supra* note 168 ("Trust remains a risky undertaking.").

[176] *See, e.g.*, Lane, *supra* note 165, at 3; Sako, *supra* note 158, at 89; Humphrey, *supra* note 23, at 217. *See also* Annette Baier, *Trust and Antitrust*, 96 ETHICS 231, 235 (1986) ("[T]rusting does require awareness of one's confidence that the trusted will not harm one, although they could harm one.").

[177] We will come back to the bases of trust in detail below, *see infra* II.D.

[178] *See also* HOFSTADTER, *supra* note 174, at 715 (Referring to the "bags-in-the-forest" example restated herein *supra* note 174 and describing this situation as follows: "Obviously, if you both leave full bags, you will both be satisfied; but equally obviously, getting something for nothing, is even more satisfying.").

[179] *See supra* note 169 and accompanying text.

as "accepted vulnerability to another's *possible* but *not expected* ill will (or lack of good will) toward one."[180]

Finally, trust in exchange relationships, as opposed to reliance as it is understood in this paper,[181] is bilateral. That means trust typically exists (if it exists) *in the other party*, while one would rely on a *third party*.

Coming back to our initial assumption,[182] it is now more apparent that in our context trust is the expectation that "things will go right". The potential transaction between a consumer and an online merchant is a typical exchange relationship entailing all the characteristics just described. Uncertainty exists as to the merchant's future behavior. In fact, the uncertainty is even greater than it is in offline transactions since the consumer might not even have any knowledge about the merchant's identity or physical location. The fact that the consumer is typically required to make an advance payment[183] puts her at risk to lose her money without subsequently getting the goods or services she paid for. The consumer bears the *risk of prior performance* referred to above.[184] It is the consumer who makes the precommitment that, according to Luhmann,

---

[180] Baier, *supra* note 176, at 235 (emphasis added).

[181] *See infra* II.B.1)b).

[182] *See supra* text following note 141.

[183] *See supra* note 93 and accompanying text.

[184] *See supra* note **Fehler! Textmarke nicht definiert.** and accompanying text.

characterizes potential trust relationships.[185] In other words, when applying Hofstadter's trader's dilemma[186] to online transactions between a merchant and a consumer, the result is that not only would the consumer often not know where to look for the merchant's bag, but also can the merchant check the consumer's bag before leaving its own (thus, it might take mine and not leave its at all). The better parallel, therefore, seems to be the typical—and highly uncomfortable—blackmail or extortion situation. I deposit my bag with the ransom in the forest and then I am at the blackmailer's mercy that she doesn't kill the hostage anyway (one might say I have to trust her, but that seems somewhat sarcastic in regard to a blackmailer). Moreover, the Internet makes it much easier for the blackmailer to pick up my bag without being trapped or identified.

In sum—unless she can rely on a third party to fix things that have gone wrong[187]—a consumer needs to have trust in a merchant is she to enter into an online transaction with it. She needs to expect the merchant not to take advantage of her exposing herself to the risk of paying in advance for goods and services that the merchant, subsequently, might or might not actually provide. To this background the most important question becomes, what these expectations, what the consumer's trust can be based upon.[188] At this point one generally very

---

[185] *See supra* note 174. For Luhmann this is a general rule. Building up trust requires a mutual commitment which will take place "in a fixed order, first the truster and then the trustee." *See id.* at 42.

[186] *See supra* note 174.

[187] We will turn to this second alternative immediately, *see infra* II.B.1)b).

[188] *See infra* II.D.

important[189] basis of trust can already be excluded: a *personal* impression of the potential trustee. In regard to non face-to-face remote transactions over the Internet, you simply cannot rely on your intuition telling you whether or not to trust someone after seeing her—because you never see her.[190] Before analyzing other possible bases of trust, however, we will first turn to its counterpart—*reliance*.

**b) Reliance**

If the consumer does not expect things to go right, that is if she does not really trust the merchant (the consumer might still *hope* that the merchant keeps its promise, but she does not really know enough; she has no sufficient basis, to *expect* it to do so) she might still enter into the transaction under the condition that she can rely on someone or some mechanism to fix things should they go wrong. Note that this was the second part of the basic assumption made earlier in this paper.[191] Sometimes reliance is used as a synonym for trust. This is, for example, the case when authors speak of an agent believing in the reliability of

---

[189] *See* GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 125 (arguing that direct personal knowledge has a higher status than, for example, media-based knowledge because it is based on a multidimensional experience allowing an impression of the whole person by seeing her, making eye contact, hearing her voice, seeing and sensing her gestures, movements, and responses etc.).

[190] *See* GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 7 (Describing personal experience as one possible basis for trust: "Often we have an intuitive sense of whom we can trust and whom not, relying on a lifetime of experience of human expressions, gestures, and character. One might say ... 'The moment I saw him, I knew I could trust him.'"). *See also* Nancy R. Furnari, *Are Traditional Agency Principles Effective for Internet Transactions, Given the Lack of Personal Interaction?*, 63 ALB. L. REV. 537, 542 (1999) (arguing that in regard to Internet transactions, with the lack of face-to-face contact, "the key element of trust is also missing").

[191] *See supra* text following note 141.

his trustee,[192] or when they ask "how far people can be relied on to do what is expected from them."[193] This is not how "reliance" will be used here. Rather, trust and reliance will be understood as counterparts and reliance is assumed to always involve a *third party or an external institution*,[194] while trust is bilateral.[195] Reliance comes into play when the basis for trust is not sufficient.[196] When I do not or cannot expect things to go right, I rely on a third party or institution to fix things should they go wrong—to *control* the partner of my transaction, to *coerce* her to keep her promise, or to afford me *redress*, preventing me from incurring a permanent loss (for example by retrieving my advance payment).[197] Reliance thus reduces the risk inherent in exchange relationships;[198] it can "compensate

---

[192] *See, e.g.*, Deakin & Wilkinson, *supra* note 158, at 147.

[193] HOLLIS, *supra* note 149, at 11.

[194] *See also* FUKUYAMA, *supra* note 145, at 341 (arguing that "[t]he moment that trust breaks down ... *third parties* [have to be] brought in to resolve differences") (emphasis added). *Cf.* NORTH, *supra* note 143, at 34 ("The greater the specialization and the number and variability of valuable attributes, the more weight must be put on *reliable institutions* that allow individuals to engage in complex contracting with a minimum of uncertainty about whether the terms of the contract can be realized. Exchange in modern economies ... necessitates institutional reliability, ....") (emphasis added); Mayer et al., *supra* note 147, at 713 (arguing that parties "don't really trust ... [i]f there are external control mechanisms that will punish the trustee for deceitful behavior").

[195] *See supra* text following note 181.

[196] *Cf.* FUKUYAMA, *supra* note 145, at 25 (Fukuyama expresses something similar when he says: "Hierarchies are necessary because all people cannot be trusted at all times to live by internalized ethical rules and do their fair share. They must ultimately be coerced by explicit rules and sanctions in the event they do not live up to them.").

[197] *Cf.* Hardin, *supra* note 149, at 624 ("[T]hat it would be in your interest to do X because the law would coerce you, would be grounds for me to rely on you—but *reliance is not trust* ...." The difference between Hardin's use of "reliance" and the use herein lies in the addressee: While Hardin would rely on you (being coerced), I would rely on the law (to coerce you).) (emphasis in the citation added).

[198] *Cf.* LUHMANN, *supra* note 168, at 34 (Luhmann asserts that "legal arrangements which lend special assurance to particular expectations, and make them sanctionable, ... lessen the risk of conferring trust.") (footnote omitted).

for an absence of trust".[199] It can, in effect, substitute trust[200] or, as Bluhm put it, "[i]f one believes that potential negative consequences can be neutralized (...), it matters little if the person with whom one is interacting is untrustworthy."[201] Instead of reliance one could certainly use terms like "control", "coercion", or simply "non-trust". But all of these terms, it seems to me, just cover specific parts of what I mean by "reliance".

### c) Some Economics of Trust and Reliance

It is frequently alleged that trust increases efficiency by reducing transaction costs.[202] Macaulay's quote of a lawyer saying that he was "sick of being told, 'We

---

[199] FUKUYAMA, *supra* note 145, at 26 (Fukuyama refers to "legal mechanisms like contracts" which, in the understanding proposed here, would be one institution to rely on in the absence of trust. In fact, it should be clarified that the mechanisms would not be just contracts, but *enforceable* contracts. Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOC. REV. 55, 56 (1963) uses the term "contract" in the latter sense when he defines it as involving "the existence or use of actual or potential legal sanctions to induce performance of the exchange or to compensate for non-performance."). *Cf.* Baier, *supra* note 176, at 251 (Baier argues that contracts offer the trusting party *security*, making it possible "to trust with minimal vulnerability." Contracts "are a device for trusting others ... without taking the risks trusters usually do take. They are designed for cooperation between mutually suspicious risk-averse strangers." I only disagree with Baier's terminology. This trust between "mutually suspicious risk-averse strangers" is not only "a limit case of trust" (*id.*) but not trust at all. It is, in the terminology used here, reliance on the contract and the possibility of its enforcement.)

[200] *See id.* at 27 (referring to the "legal apparatus, serving as a substitute for trust").

[201] Bluhm, *supra* note 33, at 338 (listing guarantees, insurance, or warranties as mechanisms that are designed to negate the unfavorable consequences which might follow from risking interaction). Something similar is expressed by LUHMANN, *supra* note 168, at 34 when he says that, "if contracts are to be trusted it is necessary that their performance be made independent of the question of who, if anybody, has in fact trusted." In other words, reliance on external institutions can make trust between the *transacting partners* irrelevant, but it may require trust in the *institution* itself (to actually be reliable). Luhmann's terminology, however, still differs somewhat from the concept proposed herein when he refers to legal regulation as the "safeguard of trust" (*id.* at 35).

[202] *See* FUKUYAMA, *supra* note 145, at 151; Sako, *supra* note 158, at 91; Deakin & Wilkinson, *supra* note 158, at 147 ("[T]rust may contribute to operational efficiency by reducing transaction costs which are associated with relational contracting.").

can trust old Max'"[203] can be understood to support that allegation (since the transaction costs are reduced on the lawyer's expense who would otherwise draft an agreement). Without trust, parties to a transaction will deal with one another only under a system of formal rules and regulations, they need to negotiate detailed contracts, which they might have to litigate and enforce.[204] This view, while pointing out the major benefits of trust, completely neglects that there are also *costs* to trust.[205] First, the trustor is at risk that her expectation as to the trustee's behavior was wrong; that the latter turned out not to be trustworthy after all. The risk inherent to trusting someone then materializes and a harm or loss is incurred. Second, there are the costs of establishing trust and assessing trustworthiness. Building trust requires time and resources to gather and verify information about the potential trustee. These two cost factors are directly related to one another. The less one invests in establishing trust and assessing trustworthiness, the greater is the risk of being wrong and incurring a loss. Even under Fukuyama's premise that a basic level of trust is inherent in any society, the need to establish trust and assess trustworthiness in regard to specific transactions remains, because, as Fukuyama himself points out, in any society

---

[203] Macaulay, *supra* note 199, at 58.

[204] *See* FUKUYAMA, *supra* note 145, at 27, 151, 200. *See also* Humphrey, *supra* note 23, at 217 ("Entering into an economic exchange exposes the agent to risks arising from the action of others. If these risks are uncontrollable, then exchange is reduced, paralysed, or rendered costly by the need to take precautions. If the 'other' can be trusted, exchange is facilitated.").

[205] The online lectures by Tamar Frankel on *Benefits, Costs and Risks to Trusting and Non-trusting*, available at <http://eon.law.harvard.edu/cgi-bin/courseware/syllabus.cgi?COURSEID=25> provided many valuable ideas for this section.

"all people cannot be trusted at all times".[206] Therefore, at least at an initial stage, it is misleading when Fukuyama asserts that trust reduces "transaction costs, incurred by activities like finding the appropriate buyer or seller".[207] At the beginning of a trust relationship there will be costs of finding the appropriate trustee. Only when the parties, once trust has been established, engage in repeated transactions with each other, will they incur less costs in these subsequent transactions. Once they turn to a new or another partner, however, they will have to bear the costs of establishing trust and assessing trustworthiness again. Thus, trust involves a relatively high investment at the beginning of the relationship, while it can make subsequent transactions between the same partners more efficient.

In regard to reliance, it is the other way round. There are no initial costs of establishing a relationship. In fact, relying on third parties or institutions to protect one from incurring a loss "allow[s] strangers with no basis for trust to work with one another".[208] On the other hand, reliance may entail relatively greater costs for each transaction, for example costs of negotiating and forming detailed contracts and, most importantly, enforcing one's rights in the event of the other

---

[206] FUKUYAMA, *supra* note 145, at 25.

[207] *Id.* at 151. *See generally* RONALD H. COASE, THE FIRM, THE MARKET, AND THE LAW 114 (1988) (Giving the classic definition of transaction costs: "In order to carry out a market transaction, it is necessary to discover who it is that one wishes to deal with, to inform people that one wishes to deal and on what terms, to conduct negotiations leading up to a bargain, to draw up the contract, to undertake the inspection needed to make sure that the terms of the contract are being observed, and so on.").

[208] *Id.* at 150 (Fukuyama, in the sentence partly cited in the text, refers to contracts. I would put a greater emphasis on the actual *enforceability* of contracts).

party's not keeping her promise.[209] These costs are the price for reducing the risk inherent to trusting.

A generalization that trust (always) increases efficiency cannot be made. Whether trust or reliance is more efficient depends on a number of factors: the costs of establishing trust, assessing trustworthiness and the risk of trusting; the costs of enforcement, coercion, or redress when relying on these means of risk prevention; and, of great importance, the number of transactions between the same partners. If the parties will engage in numerous similar transactions in the future, the up-front investment in establishing a trust relationship might pay off because of future savings in transaction costs. If the parties, however, will engage in only one or a small number of transactions, the investment in building trust might exceed the subsequent savings in transaction costs. This would make it more efficient for the parties not to invest in trust, but to rely on (in the sum relatively less expensive) means of coercion or redress in the event that things go wrong.

This also suggests, that building trust and establishing trustworthiness might have a different value for consumers and merchants, respectively.[210] A merchant

---

[209] *See generally* NORTH, *supra* note 143, at 27 (emphasizing that transaction costs "consist of the costs of measuring the valuable attributes of what is being exchanged *and the costs of protecting rights and policing and enforcing agreements*") (emphasis added).

[210] *See generally* Jay B. Barney & Mark H. Hansen, *Trustworthiness as a Source of Competitive Advantage*, 15 STRATEGIC MGMT. J. 175, 176 (1994) (perceiving of trust as the attribute of a *relationship* between exchange partners and of trustworthiness as an attribute of *individual exchange partners*); Mayer et al., *supra* note 147, at 716-724 (discussing the concept of trustworthiness the relevant factors pertaining to it). Mayer et al. also point to the difference between trust (which is understood as one person's *trusting*, as opposed to Barney & Hansen who understand it as a *trust relationship*) and *trusting behavior*. In regard to the former one does

will, by definition, engage in repeated transactions with consumers. From its point of view it does not really make a difference, who the individual consumer is. Thus, it would presumably be efficient for the merchant to establish a general impression of trustworthiness, because it might facilitate all future transactions with consumers in general. Thus, especially for merchants trustworthiness or reputation[211] is a valuable business asset.[212] The consumer, on the other hand, is not likely to deal with only one merchant, but with many different ones. So she would have to establish trust in each of these merchants. Given the fact, that the number of repeated transactions with any single merchant is limited, that might not be an efficient thing to do (because the costs of building trust in each merchant would exceed the transaction costs savings in future dealings with each of them).

Thus, before turning to bases of trust and means of reliance and to ways to enhance consumer confidence keep the following in mind. Consumer confidence and efficiency can be increased in more than one way. Enhancing trust (and

---

not need to risk anything, while the latter involves taking a risk in order to engage in a trusting action. In other words, there is a difference between "a 'willingness' to assume a risk and actually 'assuming' a risk." *See id* at 724.

[211] *See infra* II.D.3) (discussing the role of reputation in greater detail).

[212] *Cf.* KENNETH J. ARROW, THE LIMITS OF ORGANIZATION 23 (1974) ("Now trust has a very important pragmatic value, if nothing else. Trust is an important lubricant of a social system. It is extremely efficient; it saves a lot of trouble to have a fair degree of reliance on other people's word. Unfortunately this is not a commodity which can be bought very easily. If you have to buy it, you already have some doubts about what you've bought. Trust and similar values, loyalty or truth-telling, are examples of what the economist would call 'externalities'. They are goods, they are commodities; they have real, practical, economic value; they increase the efficiency of the system, enable you to produce more goods or more of whatever values you hold in high esteem. But they are not commodities for which trade on the open market is technically possible or even meaningful."). Barney & Hansen, *supra* note 210. FUKUYAMA, *supra* note 145, at 10 (arguing that

reducing the costs of establishing trust and assessing trustworthiness) is one way that might work in some cases. Reducing the costs of reliance, particularly enforcement costs, however, is another that might work in others. If, for example, the costs of reliance are sufficiently low and the costs of establishing trust are sufficiently high and if (from the consumer's perspective) a relatively small number of transactions with the same partner occurs, reliance is clearly preferable over trust (if one has to make an either/or decision). In practice the decision will to a large extent depend on which costs can be reduced more easily. Examples for both approaches will be analyzed in part III.

### *2) Enforcement and Compliance*

It has become obvious from the above that trust and reliance are closely connected to enforcement and compliance. To clarify this connection a little more, it is helpful to look in some more detail at what means of enforcement are available and at how enforcement and compliance relate to each other.

Robert Ellickson developed a system of social control in which he identifies five different sets of rules, namely personal ethics, contracts, norms, organization rules, and law. These rules are provided by five different controllers, namely the actor (first-party control), the person acted upon (second-party control), social forces (third-party control), organizations, and governments, respectively. Finally, each of these controls can employ a corresponding enforcement mechanism.

---

"trust has a large and measurable economic value"); Dasgupta, *supra* note 23, at ("[T]rust is not dissimilar to commodities such as knowledge or information.").

These are self-sanction, personal self-help, vicarious self-help, organization enforcement, and state enforcement. Altogether this leads to five combined systems of social control: self-control, promisee-enforced contracts, informal control, organization control, and the legal system.[213] Only with regard to the control system of promisee-enforced contracts, to which Ellickson assigns the enforcement mechanism of personal self-help, would I propose a slight alteration. Personal self-help, understood literally, is—subject only to very narrow exceptions in events requiring immediate action—not accepted by most modern states. If a seller refuses to deliver to a buyer what she is entitled to according to their contract, the law does not allow the buyer to take it from the seller on her own initiative. In enforcing her contract, she depends on the legal system and its institutions.[214] She will have to involve the courts and ultimately she might need state enforcement. The difference therefore, between what Ellickson calls second-party control and promisee-enforced contracts on the one hand and government control and state enforcement on the other, lies only in the initiator. State enforcement, in the sense in which it is used by Ellickson, takes place upon an autonomous decision of the state's respective authorities. "Personal self-help" takes place upon the initiative of an individual (for example a contractor) who uses—and has to use—the legal system (contract law, courts, and enforcement

---

[213] *See* ROBERT C. ELLICKSON, ORDER WITHOUT LAW 124, 131, 143 (1990). This system has been widely accepted, *see, e.g.*, NORTH, *supra* note 143, at 6, 39-40 and in fact been recognized long before Ellickson, *see* HENRY M. HART, JR. & ALBERT M. SACKS, THE LEGAL PROCESS 121-22 (1994).

[214] *But see* Edward L. Rubin, *The Nonjudicial Life of Contract: Beyond the Shadow of the Law*, 90 NW. U. L. REV. 107, 126-30 (1995) (discussing more innovative forms of self-help like taking assets as a hostage—but also emphasizing the boundaries of self-help).

authorities) as the ultimate means to enforce her rights. Since the second party's action can be based on contract or tort law I will speak of this enforcement system as *court enforcement* in general.

Understood in this way, Ellickson's system of social control reveals a dichotomy. One group, containing "personal self-help", vicarious self-help, organization enforcement, and state enforcement, is characterized by the fact that enforcement requires the involvement of a third party or institution.[215] This third party is a state authority—acting on its own initiative or on a contract promisee's, a (private) organization, or agents from the social environment. In the other "group", which includes first-party self-sanction, enforcement is completely left to its subject, in our context the contract promisor. With this dichotomy in mind, this paper will speak of *enforcement* and *compliance*,[216] respectively.

The parallel of this system to the conception of reliance and trust as laid out above now becomes more apparent. In fact, compliance is the prime *basis* of trust and the third parties or external institutions that provide for enforcement are the addressee of an agent's reliance.[217] If the consumer believes in the compliance of the merchant, she will enter into the transaction because of her trust in it. If she believes in effective enforcement in the event something goes wrong, she relies on institutions to prevent her from incurring a permanent loss.

---

[215] *See also infra* text accompanying note 215.

[216] *See also infra* note 484 (discussing compliance or *self-enforcing* contracts).

[217] *See supra* note 194 and accompanying text for the perception in this paper that reliance always involves a third party or an external institution, whereas trust is always bilateral.

But can enforcement and compliance still serve as a sufficient basis for reliance and trust—or, in short, for consumer confidence—in the online marketplace? The answer to this question will depend on whether enforcement by any of the traditional external control systems[218] is *effective* in this environment;[219] on whether and to what extent compliance can generally be expected from online merchants;[220] and on whether and how a certain level of *compliance* on the *merchants' side* will actually lead to a corresponding level of *trust* on the *consumers'* side.[221]

## C. Enforcement and Compliance in the Online-Marketplace

Above, the paper pointed out some characteristics that are peculiar to online transactions.[222] Recall some of those characteristics in the context of effective rule enforcement. First, buyers face uncertainty as to a seller's identity or actual physical location. Nothing on a website reliably indicates who is responsible for its contents and from where it is operated. In fact, sophisticated ways exist to make it virtually impossible to trace data on the web back to its point of origin (or the physical location of its originator).[223] In addition to this *anonymity*—and

---

[218] For a discussion of *new* external enforcement institutions *see infra* III.B.

[219] *See infra* II.C.1).

[220] *See infra* II.C.2).

[221] *See infra* II.D.

[222] *See supra* II.A.

[223] *See supra* text following note 115. *See also* Rothchild, *supra* note 31, at 927-28 (describing a variety of techniques to disguise one's identity in online communications).

related to it—the web is characterized by unprecedented *mobility*.[224] Online, because of the difficulties to track the physical location of a website operator, it is not necessary to abandon a physical place of business or a "boiler room,"[225] from which fraudulent telemarketing schemes are operated, when the word of the fraudulent nature of the business has spread. The fraudster merely needs to shut down its website (easy exit).[226] Escaping detection on the web is easier than ever. And because of the low entry barriers (setting up a new site requires next to no investment and can be done immediately) it is also easier than ever to continue the fraudulent activity under a slightly altered design (easy entry and low operating costs). The lack of physical assets (or the lack of knowledge regarding their whereabouts) that could otherwise be attached is another obstacle to enforcement in the online environment.[227] Finally, the Internet is characterized by an unprecedented *globality*. The perspective of reaching a global market (the FTC speaks of a "target-rich environment")[228] at very low costs[229] makes it attractive for both honest merchants and fraudsters to do their (respective) "business" online (presenting a lucrative *opportunity*). At the same

---

[224] *Cf.* FTC, *First Five Years, supra* note 106, at 4 ("In the electronic marketplace, frauds can appear suddenly, spread rapidly, and disappear without notice or warning."); Rothchild, *supra* note 31, at 926-27 (identifying and describing "portability" as one characteristic that makes it easy to evade detection).

[225] *See* Smythe, *supra* note 103, at 351 (explaining the term "boiler room" in the context of telemarketing fraud).

[226] *See supra* note 114.

[227] *See* Froomkin, *supra* note 3, at 71.

[228] *See* FTC, *New Tools of the Trade, supra* note 50, at 8.

[229] *See supra* note 114 (citing summaries why the Internet is such an attractive place to—also—do *illegitimate* business).

time it will make enforcement agencies realize the limits of their jurisdiction very quickly. In sum, the Internet may indeed present what is frequently feared to be "The Global Enforcement Challenge".[230]

### *1) Third Party Enforcement*

Recall[231] how the term enforcement is used in this paper. As opposed to compliance (or *self*-enforcement)[232] enforcement as used herein means third-party enforcement. At one point or another a third party, an external institution comes in with the power to ultimately *coerce* the party in default to compliant behavior.[233] It includes what is sometimes referred to as contract or second-party enforcement, since this also requires involvement of an external authority (courts, enforcement authorities) at some point. As has been pointed out above,[234] the difference in state enforcement and contract enforcement lies only in the actor initiating the enforcement process.

The following section will analyze whether and to what extent traditional enforcement mechanisms in each of the four control systems involving external enforcement (state enforcement, contract enforcement, organization enforcement, informal enforcement of social norms) can still provide for *effective*

---

[230] *See* ACCC, *Enforcement Challenge, supra* note 28. *See also* FTC, *First Five Years, supra* note 106, at 22 ("Cross border fraud is harder to discover and stop, redress for consumers is more difficult to achieve, ....").

[231] *See supra* note 215 and accompanying text.

[232] *See infra* note 484 and accompanying text.

[233] *See supra* note 194 and accompanying text.

[234] *See supra* II.B.2).

enforcement of consumer rights in the online environment. How can and do these mechanisms—that worked more or less well in the offline world—respond to the "global enforcement challenge" as it has just been described? The answer to this question will also tell us, whether consumers can still comfortably *rely* on these mechanisms to "fix things if they go wrong"[235] and ultimately whether they will (unless they trust the merchant)[236] enter into potentially risky distance transactions at all.

### a) State Enforcement

In market economies whose legal systems generally respect—or are, in fact, partly built on—the principles of consumer sovereignty[237] or freedom of contract[238] it is all but obvious to speak of state (initiated) enforcement in regard to individual consumers' rights. The decision whether to enter into a contract and under which terms and conditions is generally left completely to the transacting

---

[235] *See supra* note 143 and accompanying text.

[236] *See infra* II.D.

[237] *See generally* Cass R. Sunstein, *From Consumer Sovereignty to Cost-Benefit Analysis: An Incompletely Theorized Agreement?*, 23 HARV. J.L. & PUB. POL'Y 203 (1999); W. Kip Viscusi, *Using Warnings to Extend the Boundaries of Consumer Sovereignty*, 23 HARV. J.L. & PUB. POL'Y 211 (1999); Neil W. Averitt & Robert H. Lande, *Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law*, 65 ANTITRUST L.J. 713 (1997) (all discussing consumer sovereignty and whether, on what grounds, and to what extent government interference and intervention with consumer choice is legitimate). *See also* Iain Ramsay, *Consumer Protection, in* 1 THE NEW PALGRAVE, *supra* note 149, at 410, 411 (tracing the concept of consumer sovereignty to WILLIAM HAROLD HUTT, ECONOMISTS AND THE PUBLIC 257-99 (1936) who argued for the concept on the grounds of liberty of choice and toleration of a variety of individual tastes, however irrational these might be).

[238] The principle of private autonomy ("Privatautonomie") and the principle of freedom of contract ("Vertragsfreiheit") that derives from it are the fundamental basics underlying German private law. The German federal constitutional court (Bundesverfassungsgericht) has frequently emphasized that these principles are protected under art. 2(1) of the German Constitution (Grundgesetz), *see* 72 BVerfGE 155, 170; 8 BVerfGE 274, 328.

individuals. The same typically holds true for the decision whether (or when) to pursue enforcement of contractual rights or remedies when the other party does not live up to the agreement. And indeed, it would strike us not only as extremely impractical but also as unduly paternalistic[239] if governments stepped in to bring enforcement actions on behalf of a contractor every time a contract was breached. A contractor might choose not to bring such an action at all or not to bring it at this time for a variety of reasons (or for no reasons at all) and in principle one would expect the government not to interfere with this decision.

The principle of consumer sovereignty, however, is not a dogma precluding government involvement altogether. In fact, the preservation of consumer sovereignty might compel governments to step in at one point or another.[240] It is generally recognized that especially in the event of a "market failure" government interference is, to a certain extent, legitimate.[241] Expressed somewhat simplified a market failure exists either when one party to a transaction is extraordinarily strong—legitimizing government interference in the form of antitrust regulation—or when one party is extraordinarily weak—legitimizing government interference

---

[239] *Cf.* Ramsay, *supra* note 237, at 411 ("Consumer sovereignty is both an economic concept and a political slogan that is frequently contrasted with the paternalism of a 'nanny state', that restricts or channels choices.").

[240] *See id.* at 410 ("The normative goal of consumer sovereignty is the central economic rationale for consumer protection."). *See also* BVerfG, 1994 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 36, 38 (arguing that the principle of private autonomy, because it protects both partners to a contract, may indeed *demand* restrictions of the parties' freedom of contract in cases of structurally unequal bargaining power).

[241] *See, e.g.*, Timothy J. Muris, *Economics and Consumer Protection*, 60 ANTITRUST L.J. 103, 104 (1991) ("The concept of market failure can be used to support a quite conservative or quite activist consumer protection policy, depending on your bent.");

in the form of consumer protection regulation.[242] The latter can be a result of information failure, structurally unequal bargaining power, or the existence of (mostly economic) barriers to exercise existing rights.[243]

The two former of the above account for the enactment of laws aiming to protect consumers from unbalanced and unfair contracts.[244] These laws frequently require the merchant to provide the consumer with specific information prior to the formation of the contract.[245] They often afford a consumer the right to return the goods or to cancel or withdraw from the contract within a certain time period.[246] Sometimes they allow a judicial review regarding enforceability of

---

[242] *See also* Averitt & Lande, *supra* note 237 (characterizing consumer sovereignty as the "overarching unity" that connects antitrust regulation and consumer protection law). The third important basis for government interference is the protection of public policies.

[243] *See* Ramsey, *supra* note 237, at 410.

[244] *See, e.g.*, Fred H. Miller, *Consumers and the Code: The Search for the Proper Formula*, 75 WASH. U. L.Q. 187 (1997) (discussing consumer protection in the Uniform Commercial Code); William S. Mayfield, *Consumer Protection*, 13 S.U. L. REV. 279 (1987) (analyzing a number of consumer protection laws); Andreas P. Reindl, *Consumer Contracts and European Community Law*, 75 WASH. U. L.Q. 627 (1997) (giving an overview on the comprehensive activity of the European Union regarding consumer protection regulation).

[245] *See, e.g.*, Council Directive 85/577/EEC of 20 December 1985 to Protect the Consumer in Respect of Contracts Negotiated Away from Business Premises, 1985 O.J. (L 372) 31; Council Directive 87/102/EEC of 22 December 1986 for the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Consumer Credit, 1987 O.J. (L 42) 48, as amended by Council Directive 90/88/EEC of 22 February 1990, 1990 O.J. (L 61) 14, and Directive 98/7/EC of the European Parliament and the Council of 16 February 1998, 1998 O.J. (L 101) 17; Distance Contracts Directive, *supra* note 24. *See also* Pichler, *supra* note 24, at II.C.

[246] *See id. See also* FTC Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations, 16 C.F.R. § 429.1 (1999) (giving consumers a right to cancel door-to-door sales within three business dates and requiring merchants to furnish the consumer with respective notice). *See also* Mayfield, *supra* note 244, at 287-88 (referring the FTC's door-to-door sales regulation).

certain provisions in contracts, particularly of terms and conditions in standard form agreements.[247]

The latter of the reasons stated above that can lead to a consumer's structural inferiority in a transaction—the existence of (mostly economic) barriers to exercise existing rights[248] (including the rights especially granted in the consumer protection laws just described)—leads to an issue that is particularly interesting in our context: state enforcement of consumer protection laws. In this regard one can observe an interesting difference between the United States, where the enforcement of consumer protection laws to a large extent falls within the competence of the Federal Trade Commission (FTC) and the Attorneys General,[249] and Europe, where the enforcement of her rights is mostly left to the individual consumer.[250] Finally the role of criminal proceedings in this context will be addressed.[251]

#### *aa) The Federal Trade Commission and the Attorneys General*

In the U.S. the FTC and the Attorneys General act as consumer protection agencies.[252] Although expressly acknowledging the AG's role in enforcing

---

[247] *See, e.g.*, Council Directive 93/13/EEC on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) 29.

[248] The problem of consumer access to justice will be discussed in detail *infra* II.C.1)b).

[249] *See infra* II.C.1)a)aa).

[250] *See infra* II.C.1)a)bb).

[251] *See id.*

[252] For an account of important differences between the two see Muris, *supra* note 241, at 106 (noting that the FTC has considerably more resources and that the AG's are elected, leading to a

consumer's rights with regard to online commerce,[253] the following remarks will focus primarily on the FTC. According to the Federal Trade Commission Act[254] the FTC "is empowered and directed to prevent persons, partnerships, or corporations ... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[255] It has special investigative powers,[256] as well the authority to initiate an enforcement action if it finds "reason to believe" that the law is being violated.[257]

"The law" enforced by the FTC is primarily the prohibition of "unfair and deceptive acts or practices".[258] Besides that the Commission enforces a number of other consumer protection statutes that refer to its enforcement power under the FTC Act,[259] including the Truth-in-Lending Act[260] and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[261] Note, however, that the Commission's enforcement authority clearly primarily exists in the interest of the

---

tendency that the states use simple theories and seek highly visible cases, in addition to being more reluctant to expensive litigation).

[253] In fact, issues related to consumer protection in cyberspace draw increasing attention of the AG's. Stanford University, for example, was host to the National Association of Attorneys General conference on "The Impact of the Internet on the Mission of the Attorneys General" (Jan. 10-11, 2000).

[254] 15 U.S.C. §§ 41-58 (1999).

[255] *Id.* § 45(a)(2).

[256] *Id.* §§ 46, 49.

[257] *See generally* Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* (April 1998) [hereinafter FTC, *Overview*] <http://www.ftc.gov/ogc/brfovrvw.htm>.

[258] 15 U.S.C. § 45(1).

[259] For a complete overview see Federal Trade Commission, *Statutes Enforced or Administered by the Commission* (last modified July 15, 1999) <http://www.ftc.gov/ogc/stats.htm>.

[260] 15 U.S.C. §§ 1601-1667f (1999).

general public as such—or collective interests[262]—rather than in the interest of individual consumers. This explains why the enforcement authority is limited to acts or practices that "[cause] or [are] likely to cause *substantial* injury to consumers which is *not reasonably avoidable by consumers themselves* ...."[263] In determining unfairness of an act or practice, the Commission is expressly entitled to consider "established public policies".[264] This focus on collective rather than individual interests should be kept in mind when assessing the consequences of FTC enforcement on consumer reliance below.[265]

The Commission can use a number of different enforcement mechanisms. In the administrative process the Commission, if it has reason to believe that an unfair or deceptive act or practice has been used, issues a complaint stating its charges and serves it upon the alleged offender.[266] The respondent may settle the charges by consenting or contest them. The latter leads to a hearing and ultimately to a final decision and order by the commission.[267] The final order is subject to review by a court of appeals and, eventually, by the Supreme Court.[268]

---

[261] 15 U.S.C. §§ 6101-6108 (1999).

[262] This is a term which we will encounter again in the context the European Union's attempts to enhance judicial control of consumer protection laws. *See infra* II.C.1)b)bb)a□.

[263] 15 U.S.C. § 45(n) (emphasis added).

[264] *Id. See also id.* § 45(b) ("and if it shall appear to the Commission that a proceeding by it in respect thereof would be *to the interest of the public*") (emphasis added).

[265] *See infra* II.C.1)a)aa)b□bb□.

[266] 15 U.S.C. § 45(b).

[267] *See id. See also* FTC, *Overview*, *supra* note 257.

[268] *See* U.S.C. § 45(c).

If an order has become final[269] a separate suit to enforce it (by obtaining civil penalties) needs to be brought in a federal district court in the event of a violation of the order by the respondent.[270] In addition to this—and of great relevance in our context—the Commission can seek *consumer redress* in a federal district court.[271] The court in such an action may "grant such relief as [it] finds necessary to redress injury to consumers ... resulting from the rule violation or the unfair or deceptive act or practice, .... Such relief may include ... rescission or formation of contracts, the refund of money or return of property, the payment of damages ...."[272] Thus, the FTC Act actually does provide for a form of *state enforcement* that may ultimately lead to *compensation of individual consumers* who became victims of merchant fraud.[273] In this it departs from the traditional understanding of state enforcement where payments by the violator, such as criminal sanctions or civil penalties, went to the state (i.e. to the public as a whole) instead of individual victims (who normally would have had to bring their own civil action when seeking redress). As indicated above,[274] this is also an attempt to address

---

[269] For details see *id.* § 45(g).

[270] *Id.* 45(l). The penalty is up to $10,000 for each violation. Section § 45(m) also allows the Commission to bring enforcement actions against any other person (i.e. not the addressee of the initial order) who violates a Commission rule or order "with actual knowledge", prove of which normally requires that the Commission provided the violator with a copy of the order in question. *See* FTC, *Overview, supra* note 257.

[271] *See* 15 U.S.C. § 57b(a)(2). If the action is brought against an act or practice to which the Commission's cease and desist order relates (as opposed to the violation of a Commission rule) the Commission has to prove, that the act or practice is one "which a reasonable man would have known under the circumstances was dishonest or fraudulent".

[272] *See id.* § 57b(b).

[273] *See supra* note 248 and accompanying text.

[274] *See supra* note 248 and accompanying text. *See also* Muris, *supra* note 241, at 105 ("The traditional government method for enforcing those rules has been the courts. As is well known,

the problem of economic barriers for consumers to actually exercise existing rights—the problem of consumer access to justice.[275]

Instead of issuing cease and desist orders in specific cases, the FTC Act also empowers the Commission to prescribe trade rules "which define in specificity acts or practices which are unfair or deceptive".[276] Rules the Commission has prescribed under this authority include, for example, the "Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations"[277] or the "Mail Order Telephone Order Merchandise" Rule.[278] The enforcement in the event of a rule violation is parallel to the enforcement of cease and desist orders as just described. The Commission may recover civil penalties up to $ 10,000 for each violation[279] by bringing an action in a federal district court.[280] Furthermore, the Commission can bring a suit for consumer redress.[281]

However, enforcement under both these procedures is an often lengthy multiple step process. Therefore it is not surprising that another procedure, added to the

---

however, for consumer transactions going to court is usually not economically feasible. .... Thus, government consumer protection agencies have become part of the process to enforce the basic rules ....").

[275] *See infra* II.C.1)b).

[276] *See* 15 U.S.C. § 57a(1)(B).

[277] *See supra* note 246.

[278] *See* 16 C.F.R. § 435 (1999). A complete listing of the FTC's rules on commercial practices in 16 C.F.R. Ch. I is available online at <http://www.access.gpo.gov/nara/cfr/waisidx_99/16cfrv1_99.html>.

[279] Under the condition that the unfair or deceptive act or practice was undertaken "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule."

[280] *See* 15 U.S.C. § 45(m)(1)(A).

[281] *See* 15 U.S.C. § 57b(a)(1), (b).

FTC Act in 1973,[282] became the "foundation of the Commission's consumer fraud program."[283] The added Section 13(b) of the FTC Act[284] empowers the Commission, if such action would be in the interest of the public,[285] to seek preliminary injunctions in a federal district court to enjoin any act or practice that violates or is about to violate any provision of law enforced by the FTC.[286] In addition to these preliminary injunctions, which require the Commission to file a complaint within a period not exceeding 20 days, "in proper cases the Commission may seek, and after proper proof, the court may issue, a *permanent injunction*."[287] Since the early 1980's the Commission increasingly used permanent injunctions in its consumer protection program.[288] Going beyond the literary text of Section 13(b), the Commission has, in addition to permanently barring deceptive practices, also relied on this provision to obtain a freeze of assets or imposition of temporary receivers, monetary damages, and consumer redress in the form of rescission of contracts and *restitution*.[289] The courts have

---

[282] The Section was added as part of the Trans-Alaska Pipeline Authorization Act of 1973, Pub. L. No. 93-153, 87 Stat. 576. *See* Muris, *supra* note 241, at 108 n.7.

[283] Muris, *supra* note 241, at 108. Note that the term "consumer fraud" is used in the opposite sense as it is used in this paper, *see supra* note 50 (explaining the different uses of the term).

[284] 15 U.S.C. § 53(b).

[285] *See* 15 U.S.C. § 53(b)(2).

[286] *See* 15 U.S.C. § 53(b)(1).

[287] 15 U.S.C. § 53(b) (emphasis added).

[288] *See* FTC, *Overview, supra* note 257.

[289] *See id*. *See also* Muris, *supra* note 241, at 108 n.12 (citing FTC v. Atlantex Assocs., 1987-2 Trade Cas. (CCH) ¶ 67,788 (S.D. Fla. 1987), aff'd, 872 F.2d 966 (11th Cir. 1989) (ordering $12 million in consumer redress), among other cases); FTC, *First Five Years, supra* note 106, at 8-9 (giving a short description of the FTC's enforcement actions under Section 13(b) of the FTC Act).

accepted this construction of the Section by the Commission.[290] Making use of permanent injunctions and seeking redress under this procedure has many advantages over traditional administrative action in the form of cease and desist orders. It is namely faster and becomes effective immediately, and the Commission can seek prohibitory and monetary relief in one single step. Thus, "most consumer protection enforcement is now conducted directly in court under Section 13(b), rather than by means of administrative adjudication."[291] In our context it is worthy to repeat that Section 13(b) has successfully (i.e. with approval of the courts) been construed by the Commission as to including an authorization to seek *consumer redress* in addition to stopping the unfair or deceptive conduct.

*α) Enforcement Efforts Regarding Electronic Commerce*

As of December 15, 1999 the FTC has brought more than 100 enforcement actions involving the Internet and online services.[292] Since the very beginning it has been the Commission's declared policy that consumer protection principles be applied in the electronic marketplace no less than they are offline.[293] But the FTC has also taken new approaches to take on the challenges for consumer

---

[290] *See id.*

[291] *See* FTC, *Overview, supra* note 257. *See also* Muris, *supra* note 241, at 109 n.14 (explaining the lengthy process of first obtaining a final cease and desist order and then bringing a separate proceeding under 15 U.S.C. § 57b(a)(2) seeking consumer redress).

[292] *See* FTC, *Cases, supra* note 125.

[293] *See* Federal Trade Commission, Staff Report, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* 46 (May 1996) <http://www.ftc.gov/opp/global/report/gc_v2.pdf> [hereinafter FTC, *Anticipating the 21st Century*].

protection presented by the new and rapidly changing online environment.[294] Believing that to some extent "the answer to the machine is in the machine"[295] the Commission established "Consumer Sentinel", a database containing consumer fraud complaints—contributed by consumers,[296] law enforcement agencies, or consumer organizations like the Better Business Bureau. The data can be retrieved by various law enforcement agencies in the U.S. and Canada.[297] This initiative tries to address the problem of sharing a lot of information very fast, which is crucial to fight frequently transient[298] Internet fraud schemes. Since learning of fraudulent online practices is not enough, the Commission also created an Internet Fraud Rapid Response Team, that puts particular matters on a fast track for enforcement.[299] The Commission further established an Internet

---

Other policy goals included avoiding undue burdens on business and technology, encouraging effective self-regulation, and fostering co-operation between the public and the private sector.

[294] *See generally* FTC, *The Challenge and the Campaign, supra* note 50; FTC, *New Tools of the Trade, supra* note 50; FTC, *First Five Years, supra* note 106 (all describing the challenges faced and the new approaches taken by the Commission to address them). *See also* WORKING GROUP II, *supra* note 4, at 18-20 (describing the FTC's and other agencies' efforts).

[295] *See generally* Charles Clark, *The Answer to the Machine is in the Machine, in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 139 (P. Bernt Hugenholtz ed., 1996) (coining this expression in regard to law enforcement and cyberspace).

[296] Via the FTC's tell-free telephone number, or by using the online complaint form. *See* Federal Trade Commission, Bureau of Consumer Protection, *Complaint Form* (last modified Feb. 18, 2000) <https://www.ftc.gov/ftc/complaint.htm>. *See also* FindLaw Legal News, *U.S. launches Internet fraud complaint center* (May 8, 2000) <http://news.findlaw.com/legalnews/s/20000508/N0848641.html> (quoting Attorney General Janet Reno: "It will be a one-stop shopping approach to identifying Internet fraud schemes and referring them to the proper law enforcement agencies.").

[297] *See* FTC, *First Five Years, supra* note 106, at 4-5.

[298] *See supra* note 224 and accompanying text.

[299] *See* FTC, *First Five Years, supra* note 106, at 5 (citing FTC v. Benoit, No. 3:99 CV 181 (W.D.N.C. filed May 11, 1999), a case in which an injunction stopping the deceptive conduct was reached within three weeks of learning about it).

Lab providing the necessary state-of-the-art equipment and developing the necessary expertise to effectively investigate online.[300]

It further introduced so called "Surf Days", a combined and concentrated effort by several law enforcement agencies focusing on identifying specific online scams.[301] The identification of questionable conduct is followed by a warning to the site operators, in response to which many of whom improve or remove their sites,[302] a follow-up visit, and eventually enforcement action if the site operator has not responded.

In addition to enforcement the FTC emphasizes business and consumer education, disseminating information over the web and thus making use of the "target-rich environment"[303] for its own purposes this time.[304] Another tool employed by the Commission is the "teaser" website.[305] These sites are designed to mimic fraudulent sites and are indexed in a way that they are as likely to be found by search engines as their "original" counterparts. After leading the user through several steps, the FTC seal appears and warns the user that

---

[300] *See id.*

[301] *See id.* at 6; FTC, *New Tools for the Trade, supra* note 50, at 12. The Commission's efforts included a Credit Repair Surf Day, a Business Opportunities Surf Day, a Scholar Scam Surf Day, a Coupon-related Business Opportunity Surf Day, an International Health Claims Surf Day, a HUD Tracers Surf Day, an International Surf Day, a Health Claims Surf Day, a Pyramids Surf Day, a Business and Investment Opportunities Surf Day, and Junk Email Surf Day. *See* FTC, *New Tools for the Trade, supra* note 50, at 13-14; FTC, *First Five Years, supra* note 106, at 6.

[302] Although there seems to be no control as to how many of them just *redesign* their sites. *See supra* note 115 and accompanying text regarding the problem of redesigning and "reopening" fraudulent sites.

[303] *See supra* note 228.

[304] *See* FTC, *First Five Years, supra* note 106, at 16.

offers like this one are often fraudulent. The idea behind it basically is to reach consumers before fraudsters do and to raise their awareness.[306] The educational efforts finally include partnerships with reputable and popular online services and other entities that link to FTC information, and consumer.gov,[307] an easy to understand site featuring tips and information for consumers.[308]

These efforts by the Federal Trade Commission and other enforcement agencies are certainly very valuable and without doubt they play a significant role in reducing online fraud. Just how significant that role is, however, remains unclear. The next section will discuss the obvious limits of state enforcement in the context of online commerce and their implications for consumer reliance on this kind of enforcement.

### *β) The Limits of State Enforcement and Their Implications for Consumer Reliance*

An increased effort by the FTC and other state enforcement agencies to enforce consumer protection laws in cyberspace will likely make the Internet a *safer*, but almost certainly not a *safe* place for consumers. As in other areas,[309]

---

[305] *See id.*

[306] *See* FTC, *New Tools of the Trade, supra* note 50, at 18.

[307] *See* <http://www.consumer.gov>.

[308] *See* FTC, *First Five Years, supra* note 106, at 17.

[309] Despite increased enforcement efforts, for example, against telemarketing fraud—the Telemarketing and Consumer Fraud and Abuse Prevention Act, *supra* note 261, was passed by Congress in 1994 as Pub. L. No. 103-297 and as directed in the Act the FTC promulgated the Telemarketing Sales Rule, 16 C.F.R. § 310 (1999), effective Dec. 31, 1995—telemarketing fraud itself evolved with it, *see* FTC, *The Challenge and the Campaign, supra* note 50, Executive Summary.

enforcement won't be perfect. And even more than in other areas, there will be a constant race between new, more sophisticated, and harder to detect online scams and improved law enforcement. As mentioned before, the Internet provides enormous opportunities for fraudsters.[310] These are combined with chances of escaping detection that are greater than ever.[311] To this background it appears fair to assume that Internet fraud is here to stay—and grow.

*αα)* *Limited Enforcement*

Recall some of the major challenges for law enforcement in this new environment that have been identified earlier: *anonymity, mobility* and *globality*.[312] The first two make it hard to detect and trace fraudsters. "[M]astering the technology and finding the perpetrators in cyberspace" is concededly a significant problem faced by the FTC and other law enforcement agencies.[313] The fact that, while fraud is increasing, "government resources at all levels are shrinking",[314] presents an additional problem. To be sure, law enforcement agencies will also make use of the newest technology, they will develop considerable expertise,[315] and they will

---

[310] *See supra* notes 114 and text accompanying notes 228-229.

[311] *See supra* II.C.

[312] For a general overview *see supra* II.C.

[313] *See* FTC, *New Tools of the Trade, supra* note 50, at 5. *See also* FTC, *The Challenge and the Campaign, supra* note 50, Challenges for Law Enforcement ("The increase in high-tech and global marketing scams is especially troublesome."); FTC, *Anticipating the 21st Century, supra* note 293, at 4 ("For law enforcement agencies, the emerging technologies present serious challenges in detection, apprehension, and enforcement. With a telephone or an online link, fraudulent marketers can set up shop quickly and cheaply, and move on without a trace. ... For the cyber scam artist, it may be even easier [than for the fraudulent telemarketer] to escape detection.").

[314] *See* FTC, *Anticipating the 21st Century, supra* note 293, at 5.

[315] *See supra* note 300 (referring to the FTC's Internet Lab).

increasingly co-operate with Secret Service, other government agencies, and the private sector to detect and trace online fraud.[316] On the other hand it is obvious, that the fraudsters' expertise in concealing their identity and location and avoiding detection will increase as well.[317] Moreover, legitimate privacy interests[318] of honest users will establish yet other boundaries for the investigative powers of law enforcement agencies.[319]

Put these problems of tracing a fraudster aside for a moment, and take one step back: Thinking about how to trace a fraudster presupposes that the enforcement agency *knows* about the fraud in the first place. The sheer magnitude of online communication suggests that a significant number of fraudulent communications will remain undetected. The "Surf Days"[320] established by the FTC would not help to detect fraudulent schemes that are not apparent from the website itself. In particular they won't allow detection of merchants that take orders (and money) but never send the goods to the consumer. Detecting those scams would require test orders, a process that may be lengthy and cannot feasibly be done on a large scale. Thus, enforcement agencies depend on consumers' reporting a

---

[316] *See* FTC, *New Tools of the Trade, supra* note 50, at 5 (citing FTC v. Audiotex Connection, Inc., CV-97-0726 (E.D.N.Y. filed Feb. 13, 1997) and describing how co-operation with AT&T and Secret Service helped to find the scammers and their assets).

[317] *See supra* note 223.

[318] Including a legitimate interest in anonymity, *see, e.g.*, Rothchild, *supra* note 31, at 928.

[319] The conflict of legitimate interests in privacy with the interests of law enforcement agencies have been discussed intensively, in particular to the background of the U.S. encryption policy. *See also* Jake Kirchner, *Forget having privacy on the Net*, ZDNet News (March 22, 2000) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2472006,00.html> (citing cases giving "scary" evidence "of a rush by police, judges, and legislators to take advantage of new technologies with little or no thought to the privacy issues involved).

fraud. Given the fact, however, that an overwhelming number of consumers never report being defrauded,[321] this is a highly unsatisfactory basis for detecting fraudulent practices of online merchants.

Finally, even when law enforcement agencies learned of a fraudulent practice *and* were able to trace the perpetrator, they may—and in the online context they will *increasingly*—face jurisdictional limits.[322] As a general principle of international law, a sovereign's (or its agencies') jurisdiction to enforce[323] is strictly limited to its own territory to the extent that a state's authorities cannot directly exercise physical power in another state's territory without that state's consent.[324] Accordingly, Section 3 of the FTC act expressly states that "[t]he

---

[320] *See supra* note 301 and accompanying text.

[321] *See* FTC, *The Challenge and the Campaign, supra* note 50, n.23 and accompanying text (citing the FTC's Project Roadblock, revealing that less than five percent of consumers affected by deceptive practices reported their losses). *See also* Committee on Government Operations, *The Scourge of Telemarketing Fraud: What Can Be Done Against it?*, Fifteenth Report by the Committee on Government Operations (U.S. G.P.O.: 1991), p.2 (estimating that less than one-tenth of consumer victims of telemarketing fraud ever report their victimization).

[322] *See also* Heckman, *supra* note 113, at 2.4 ("Even if law enforcement can identify and locate a fraudulent supplier, successful apprehension and prosecution will often depend on co-operation from multiple jurisdictions.").

[323] *See generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401 (1986) (The Restatement distinguishes between jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce as follows: "Under international law a state is subject to limitations on (a) jurisdiction to prescribe, i.e., to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or regulation, or by determination of a court; (b) jurisdiction to adjudicate, i.e., to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the state is a party to the proceedings; (c) jurisdiction to enforce, i.e., to induce or compel compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.").

[324] The prohibition of exercising physical power within the territory of another sovereign is a long standing and undisputed principle of the law of nations. *See, e.g.*, S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18-19 (Sept. 7) ("Now the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is

commission may prosecute ... any inquiry necessary to its duties *in any part of the United States*."[325] To be sure, a state is not generally barred from *ordering* enforcement measures against foreigners.[326] Thus, a court or an administrative agency—if it has the respective competence under domestic law—could in principle impose civil or criminal sanctions or penalties, order a person to refrain from doing specific acts, or order a freeze of assets[327] pertaining to persons (or assets) located outside its territory. But *actual enforcement* of these orders would always require recognition of the measures and cooperation by the respective foreign state. Moreover, it is dubious whether the FTC could even initiate the respective orders in the first place, since the FTC Act expressly limits its authority to inquiries *in any part of the United States*.[328]

---

certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.").

Jurisdiction to prescribe and jurisdiction to adjudicate are not in the same sense strictly territorial, since they may also be exercised in regard to conduct that takes place in a foreign country but has certain *effects* within the U.S. *See generally* Rothchild, *supra* note 31, at 912-915 (discussing jurisdiction to prescribe and to adjudicate in the online context).

[325] 15 U.S.C. § 43 (1999) (emphasis added).

[326] In this regard the term "jurisdiction to enforce" as used in the RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 431 (1986) is broader than the prohibited exercise of a state's power in any form in the territory of another State. According to Section 431(3) "A state may employ enforcement measures against a person located outside its territory (a) if the person is given notice of the claims or charges against him that is reasonable in the circumstances; (b) if the person is given an opportunity to be heard, ordinarily in advance of enforcement, whether in person or by counsel or other representative; and (c) when enforcement is through the courts, if the state has jurisdiction to adjudicate."

[327] *See, e.g.*, Hong Kong and Shanghai Banking Corporation v. Simon, 153 F.3d 991, 996 (9th Cir. 1998) (freeze of assets not located in jurisdiction in bankruptcy proceedings).

[328] *See supra* note 325. According to RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 431(1) (1986) "A state may employ judicial or nonjudicial measures to induce or compel compliance or punish noncompliance with its laws or regulations, provided it has jurisdiction to prescribe in accordance with ss 402 and 403." And although Congress generally has the power to extend the scope of legislation extraterritorially when a sufficient connection to the U.S. exists, "[i]t is a long-standing principle of American law 'that legislation of Congress, unless a contrary intent appears,

To this background it is not surprising that the FTC itself sees globalization and "cross-border fraud" as the major challenges in the online arena.[329] As described above, actual enforcement in a foreign country always requires cooperation of the respective authorities in that state.[330] While this might work out well in some cases,[331] it probably will not in others,[332] and it will almost always be more time consuming.

In sum, state enforcement faces considerable obstacles in the online environment. It will constantly have to try to catch up with perpetrators, and it will never be able to completely overcome the problems posed by *anonymity, mobility*, and *globality*—the three main characteristics that are inherent to cyberspace and that are so advantageous to online fraudsters.

---

is meant to apply only within the territorial jurisdiction of the United States.'" *See* EEOC v. Arabic American Oil Co., 499 U.S. 244, 248 (1991) (quoting Foley Bros. v. Filardo, 336 U.S. 281, 285 (1949)). The language in the FTC Act ("in any part of the United States"), however, strongly indicates that the Act was *not* meant to be applied extraterritorially.

[329] *See* FTC, *First Five Years, supra* note 106, at 22; FTC, *The Challenge and the Campaign, supra* note 50. *See also supra* note 230.

[330] *See also* ACCC, *Enforcement Challenge, supra* note 28, at 30, 36. There are also increased efforts to cooperate with regard to the *detection* of online scams, *see, e.g.*, Federal Trade Commission, *150 Organizations in 28 Countries Tackle Internet Fraud* (March 23, 2000) <http://www.ftc.gov/opa/2000/03/rich.htm> (describing an international surf day as "the largest ever international law enforcement project to fight fraud on the Internet").

[331] *See, e.g.*, FTC v. Carlos Pereira d/b/a atariz.com, No. 99-1367-A (E.D. Va filed Sept. 14, 1999) (involving close cooperation between the FTC and the Australian Competition and Consumer Commission, *see* FTC, *Cases, supra* note 125, at 40). *See also* FTC, *New Tools of the Trade, supra* note 50, at 16 (describing the "internic.com" case—*see supra* note 117—that involved an Australian site operator and was ultimately referred by the FTC to the Australian Competition and Consumer Commission, which is now investigating the case).

[332] In fact, there already seem to be some countries establishing themselves as a preferred base for fraudulent activities aimed at "foreign" consumers.

### *ββ) Limited Reliance*

Those limits to state enforcement, the fact that it will always be far from perfect, however, is just one reason why it will not really induce *individual consumers* to confidently rely on it when deciding whether to enter in potentially risky online transactions. Unless when trusting the merchant, the consumer will generally enter into transactions only if she believes that things can be fixed if they go wrong—if she can *rely* on an external institution to prevent her from incurring a permanent loss. Besides necessarily being imperfect, i.e. not being able to detect, trace, or bring enforcement actions against all fraudulent online merchants, there are several other reasons why consumers are likely *not* to rely on state enforcement—and in fact would be ill-advised to do so.

First, recall that state enforcement agencies primarily act in the interest of the public as a whole, rather than in the interest of individual consumers. This general principle is expressed in the FTC Act, which calls on the Commission to issue a complaint in regard to unfair or deceptive acts or practices "if it shall appear to the Commission that a proceeding by it in respect thereof would be *to the interest of the public*".[333] It has also been mentioned before[334] that the Commission's authority is limited to acts or practices that "[cause] or [are] likely to cause *substantial* injury to consumers which is *not reasonably avoidable by*

---

[333] 15 U.S.C. § 45(b) (emphasis added). *See also supra* note 264 and accompanying text. Preliminary or permanent injunctions—the main enforcement procedure employed by the Commission in consumer protection cases—will also only be granted if it "would be in the interest of the public." *See* 15 U.S.C. § 53(b)(2).

[334] *See supra* text accompanying note 263.

*consumers themselves* ....”[335] This could, above all, have an impact on the Commission’s allocation of resources, which are likely to be devoted to cases affecting a large number of victims.[336] Thus, the victim of a relatively “small” but may be hard-to-detect scam, runs a great risk of being disappointed when relying on the FTC to step in on her behalf. And consumers who become victims of scams typically don’t know that in advance (i.e. when entering the transaction). That means they neither know whether things will go wrong at all, nor do they know for how many people they will if they do. Altogether this brings about a fair degree of uncertainty whether state enforcement agencies, given the problem of limited resources, will find that taking action *in a particular case* will be to the overall interest of the public or not—and consumers virtually have no way to find out in advance. And remember that this uncertainty exists *in addition* to the uncertainties as to whether the Commission—even if it decided to bring an enforcement action—will be able to *identify* the fraudster, *track* her, and find her within its *jurisdictional reach*.

To be sure, although the FTC acts primarily in the public interest, it is empowered to bring actions for consumer redress.[337] In fact, without that possibility there would be no basis for consumer reliance at all, since a civil penalty[338] and

---

[335] 15 U.S.C. § 45(n) (emphasis added).

[336] *See also supra* note 252 (citing Muris arguing that State Attorney Generals, who are elected, are likely to choose highly visible cases).

[337] *See supra* notes 271, 281, and 289 and accompanying text (describing the availability of consumer redress under all enforcement procedures—cease and desist order, rule violation, injunctions—available to the Commission).

[338] Just as a criminal sanction, *see infra* II.C.1)a)bb).

stopping the fraudulent behavior for the future might protect *potential future victims*, but does not fix things for the consumer for whom they *already* have gone wrong. But the latter—the availability of recourse or redress if she doesn't get the goods and services she paid for—is, of course, an individual consumer's main concern when deciding whether to enter into a transaction or not.[339] So the FTC's power to seek consumer redress is a prerequisite to establishing *any* basis for consumer reliance. Redress, however, is not available unless the Commission detects the fraud, decides to take action, identifies the fraudster, tracks her location, and has jurisdiction to bring enforcement action against her.[340] Thus, it is subject to the same limitations that have been discussed above. In addition to these, there are at least two more obstacles specifically related to consumer redress sought by the Commission. First, unless a fraudster keeps perfect records, it might prove very difficult to identify all consumers victimized by a specific fraudulent, unfair, or deceptive act. And given the phenomenon of widespread underreporting,[341] one cannot expect all victims to monitor FTC actions or the respective public notices to learn about enforcement actions and the possible availability of redress.[342] Thus, the Commission might not know

---

[339] *See supra* notes 15, 144 and accompanying text.

[340] To be sure, the FTC does seek redress "for all injured consumers, no matter where they live", *see* FTC, *First Five Years, supra* note 106, at 23. This, however, only works when the perpetrator can be found within the FTC's jurisdiction. If that is not the case, the FTC might be unable to even seek redress for consumers within the U.S.

[341] *See supra* note 321.

[342] *See* 15 U.S.C. § 57b(c)(2) ("The court shall cause notice of an action under this section [for consumer redress] to be given in a manner which is reasonably calculated, under all of the circumstances, to apprise the persons ... allegedly injured by the defendant's rule violation or act or practice of the pendency of such action. Such notice may, in the discretion of the court, be given by publication.").

about all victims, and the victims might not know about the FTC seeking redress on their behalf. In both cases consumers won't get redress after all. Also, the Commission can't guarantee that at the time redress is sought it will be able to find sufficient assets to redress all the victims.[343] In fact, sophisticated fraudsters are likely to find ways to keep their profits out of law enforcement's reach.

Finally, the FTC's authority is limited to "*unfair* or *deceptive* acts or practices in or affecting commerce".[344] This means that the FTC does not step in, when—absent an actually deceptive or fraudulent act of the merchant—things "just go wrong", as they do from time to time in cross-border transactions.[345] The fact that it will not always be easy to tell, why goods in such transactions never arrived (and the fact that it will be even harder to proof why they didn't) adds to the uncertainty as to whether state enforcement will eventually step in or not. Did the goods not arrive because the merchant, as it has planned from the very beginning, never sent them, or because they just got lost in transit? The former could trigger FTC action, while the latter would not.

It is not the intention of this paper to belittle or even deny the importance of the FTC's actions in regard to protecting consumers online. There can hardly be any doubt, that these actions reduce online fraud and make the online marketplace a

---

[343] For an example see FTC, *New Tools of the Trade, supra* note 50, at 11 (citing a case in which the FTC filed suit against a perpetrator and obtained an asset freeze over $1.4 million—defrauded consumers, however, spent a total of $9.5 million).

[344] 15 U.S.C. § 45(a)(2) (emphasis added). *See also supra* text accompanying note 255.

[345] *See supra* note 122 and accompanying text. Heckman, *supra* note 113, at 2.4 calls this "more innocent violations of consumer protection regulation."

generally somewhat safer place for consumers. But there can also be no doubt, that the Commission's enforcement actions will stay far from eliminating online fraud. The Commission and other state enforcement agencies will not be able to detect all fraudulent actions, bring action even against all that are detected, identify all persons behind them, track the physical location of those persons, actually assert jurisdiction over them, or recover all losses incurred by consumers. And, most importantly, it is impossible for an individual consumer to tell ex ante whether she will ultimately get redress by state enforcement if things go wrong in *that one transaction* she is or isn't about to enter. One simply cannot know in advance. Therefore state enforcement remains important, but it is next to *no basis for consumer reliance*.

### *bb) The European Approach and Criminal Proceedings*

While the FTC acts primarily in the interest of the public in general, it may also seek consumer redress under specific circumstances. When a merchant's online act or practice reaches the quality of a criminal offense, the merchant may also face criminal enforcement actions. The remedies under criminal law generally contain fines and penalties. It does not provide for redress for individual consumers. It is, in fact, usually left to the victim to seek compensation in a separate civil action for breach of contract or fraud.[346]

---

[346] *See also* Ellen M. Faro, Note, *Telemarketing Credit Card Fraud: Is RICO one Answer?*, 1990 U. ILL. L. REV. 675. Faro asserts that, regarding credit card fraud, the present criminal laws are not an effective deterrent. She proposes to give victims more incentives to combat credit card fraud by means of civil suits for damages that go beyond actions under theories of ordinary common law fraud. She namely proposes to apply the Racketeer Influenced and Corrupt

Thus, subject to and within the same limitations identified in regard to enforcement by the FTC (difficulties to detect fraud, identify fraudsters, assert jurisdiction over them, etc.),[347] criminal enforcement may serve as a general deterrent against deceptive or fraudulent online practices. But absent a possibility to seek redress for individual consumers, it cannot serve as a basis for consumer reliance, because criminal law simply can't "fix things" for the consumer for whom they have already gone wrong.

European countries have no equivalent to the FTC. Enforcement of consumer protection laws or of consumer rights is generally left to the consumers who must bring civil actions in the courts if they desire redress.[348] The European Commission itself rightly points out that "European Directives generally aim to give (through their implementation) direct rights to consumers, which they can invoke against enterprises and professionals. Any failure or difficulty in guaranteeing access to justice to individual consumers automatically leads to

---

Organizations Act of 1970, Pub. L. No. 91-452, § 901(a), 84 Stat. 941 (codified at 18 U.S.C. §§ 1961-68 (1999) [hereinafter RICO]), under which victims may bring a civil action in a United States district court to recover treble damages and reasonable attorney's fees (*see* 18 U.S.C. § 1964(c)).

For a discussion whether RICO, which was originally meant to combat organized crime, applies to so called "garden variety" fraud see, for example, Faro, *supra*, at 686; Note, *Civil RICO and "Garden Variety" Fraud—A Suggested Analysis*, 58 ST. JOHN'S L. REV. 93 (1983); Comment, *Civil RICO and Its Application to "Garden Variety" Fraud Within the Sixth Circuit*, 13 N. KY. L. REV. 463 (1987); Comment, *What Have They Done to Civil RICO: The Supreme Court Takes the Racketeering Requirement Out of Racketeering*, 35 AM. U. L. REV. 821 (1986).

[347] *See supra* II.C.1)a)aa)b□aa□.

[348] *See also supra* note 274.

failures in the enforcement of European law at the national level."[349] Having shown the limits of state enforcement, we will now turn to *court enforcement* (and the problem of access to justice for individual consumers) to see whether it provides a viable basis for consumer reliance in the context of electronic commerce.

### b) Court Enforcement

Court enforcement typically refers to a civil action for breach of contract or fraud brought by the consumer who did not get what she paid for or was defrauded in another way.[350] In addition to that there are some less traditional variations of court enforcement like rights to sue for consumer organizations[351] or class actions. These alternatives will immediately be addressed in greater detail. One problem, however, is common to all of these options as well as to state enforcement. For practical reasons, a suit against a merchant can't be brought if that merchant can't be *identified* nor *located*. In this respect court enforcement faces the same problems (particularly anonymity and mobility) that have been discussed above in the context of state enforcement.[352] When concealing its identity and escaping detection it makes no difference for a fraudster whether she is concealing it from or escaping a government agency or a defrauded

---

[349] *See* European Commission, *Working Paper on Enforcement of European Consumer Legislation* 14 (visited Aug. 17, 00) <http://www.europa.eu.int/comm/dg24/policy/developments/enfo/enfo01_en.pdf>

[350] *See infra* II.C.1)b)aa).

[351] *See infra* II.C.1)b)bb).

[352] *See supra* II.C.1)a)aa)b□aa□.

consumer. This already presents a significant limitation for court enforcement as a basis for consumer reliance. But even when the potential defendant can be identified and located, the possibility of court enforcement is unlikely to generate significant consumer confidence  in the fact that things can be fixed if they go wrong—that it is safe to rely on the *actual* availability of redress to compensate losses that have been incurred. The following sections will analyze this for the different alternatives of court enforcement mentioned above.

### *aa) Suits Brought by Individual Consumers*

It is one thing that a consumer has the *right* to bring a suit against a merchant who not fully complied with its obligations or engaged in fraudulent activities. It is another thing, whether consumers will actually do so *in practice*—whether it makes economic sense for a consumer to do so.

#### *α) Some Economics of Consumer Litigation*

As a general rule,[353] a rational plaintiff will bring suit if and only if the expected judgment exceeds her expected litigation costs. The expected judgment is the

---

[353] On the economics of litigation *see generally* William M. Landes, *An Economic Analysis of the Courts*, 14 J. LAW & ECON. 61 (1971); John P. Gould, *The Economics of Legal Conflicts*, 2 J. LEGAL STUD. 279 (1973); Richard A. Posner, *An Economic Approach to Legal Procedure and Judicial Administration*, 2 J. LEGAL STUD. 399 (1973); Steven Shavell, *Suit, Settlement, and Trial: A Theoretical Analysis Under Alternative Methods for the Allocation of Legal Costs*, 11 J. LEGAL STUD. 55 (1982) [hereinafter Shavell, *Suit, Settlement, and Trial*]; Steven Shavell, *The Social Versus The Private Incentive to Bring Suit in a Costly Legal System*, 11 J. LEGAL STUD. 333 (1982) [hereinafter Shavell, *Incentive to Bring Suit*]; Robert D. Cooter & Daniel L. Rubinfeld, *Economic Analysis of Legal Disputes and Their Resolution*, 27 J. ECON. LIT. 1067 (1989); Lucian Arye Bebchuk, *A New Theory Concerning the Credibility and Success of Threats to Sue*, 25 J. LEGAL STUD. 1 (1996); Lucian Arye Bebchuk & Howard F. Chang, *An Analysis of Fee Shifting Based on the Margin of Victory: On Frivolous Suits, Meritorious Suits, and the Role of Rule 11*, 25 J. LEGAL STUD. 371 (1996). *See also* A. MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND

judgment in favor of the plaintiff when she wins the case multiplied by the probability of winning.[354] If the conditions are reversed, a rational plaintiff will not sue. She would incur higher costs than she would benefit from her expected judgment. Her net benefits would be negative; she would lose money. These so called "negative-expected-value suits" are common in small-stakes cases[355] and lead to a general problem of access to legal remedies when the plaintiff's claim is small in relation to the costs.[356]

*αα) Benefits*

Due to the nature of business-to-consumer transactions, the stakes involved are typically relatively low. In one survey of consumer purchases, for example, the average value of goods involved in a transaction was about $40.[357] The overall average of value per transaction is presumably even lower than that. So even when the plaintiff's probability of prevailing at trial were one, the expected judgment would be quite low.[358]

---

ECONOMICS 107-18 (2d ed. 1989); RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW § 21.5, at 607-15; § 21.9, at 624-32 (5th ed. 1998).

[354] When p is the probability of the plaintiff winning, J the value of a winning judgment, and c the costs then the plaintiff would sue if pJ > c.

[355] *See* Bebchuk, *supra* note 353, at 1-2. *See also* Cooter & Rubinfeld, *supra* 353, at 1089.

[356] *See, e.g.*, Posner, *supra* note 353, at 438; POSNER, *supra* note 353, § 21.9, at 627.

[357] *See* Stiftung Warentest, *supra* note 131, at 24.

[358] In this value range, even treble damages under RICO (*see supra* note 346) would not significantly change that fact.

The probability of winning, however, generally is not one. It is, among other things, influenced by the possibility of judicial error.[359] Some authors have shown a connection between the frequency of judicial error, the parties' expenditures on litigation and the stakes involved in the dispute. The resource inputs by the plaintiff and the defendant raise or lower the probability of the plaintiff winning the case, respectively[360]—at least to some extent.[361] The resource inputs themselves are influenced by the stakes. Higher stakes will induce the parties to spend more money on litigation, which will in turn reduce the probability of judicial error.[362] This suggest that the probability of winning tends to be lower[363] when the asserted claim is relatively small—as it typically is in the business-to-consumer transactions discussed here. There are some other factors that influence the probability of prevailing in court and that are particularly problematic in the context of disputes resulting out of e-commerce transactions. Often the consumer will lack information or documentation regarding the transaction and the merchant's conduct. Thus, although she clearly was defrauded, she might have a hard time proving her case. Moreover, in an action for fraud, the plaintiff

---

[359] *See* A. Mitchell Polinsky & Steven Shavell, *Legal Error, Litigation, and the Incentive to Obey the Law*, 5 J. L. ECON. & ORG. 99 (1989).

[360] *See* Landes, *supra* note 353, at 101. *See also* Gould, *supra* note 353, at 287 (describing the decision as to the amount of resources each party will spend as a two-person game in which the optimal expenditure of one litigant depends on the behavior of the other)

[361] *See* Posner, *supra* note 353, at 435 (suggesting a threshold above which the outcome of litigation is possibly insensitive to variations in the parties' expenditures).

[362] *See id.*, at 404, 429-435, 441.

[363] While augmenting it by increased litigation expenditure faces the limits set by inequality (1).

must comply with Rule 9(b) of the Federal Rules of Civil Procedure,[364] requiring that "[i]n all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity."[365] As construed by the courts in light of Rules 8(a)(2),[366] 8(e)(1),[367] and 8(f),[368] "[i]n order to meet the requirements of Rule 9(b), the complaint must identify the time, place, content, and maker of the false representation."[369] These requirements have proven problematic in mail and wire fraud cases,[370] and the same danger obviously exists in the online context.

Further, e-commerce transactions are often international.[371] Cross-border litigation frequently raises difficult choice of law issues. Courts and parties might face the question whether clickwrap choice-of-law clauses are enforceable and the preliminary question, which law governs the enforceability question. These issues can have a substantial influence on the outcome of the case, since different views prevail, for example, on the enforceability of warranty disclaimers

---

[364] *See also* Faro, *supra* note 346, at 689 (pointing to that problem in regard to wire fraud violations, "because the details of the telephone uses are generally only within the possession of the defendant"). For an overview on whether courts will allow discovery in these cases see *id.* at 696-98.

[365] *See* FED. R. CIV. P. 9(b).

[366] " A pleading which sets forth a claim for relief ... shall contain ... a short and plain statement of the claim showing that the pleader is entitled to relief, ...."

[367] "Each averment of a pleading shall be simple, concise, and direct. No technical forms of pleading or motions are required."

[368] "All pleadings shall be so construed as to do substantial justice."

[369] *See* Faro, *supra* note 346, at 689 (citing Haber v. Kobrin, [1982-83 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 99,259, at 96,161 (S.D.N.Y. June 3, 1983); Bennett v. Berg, 685 F.2d 1053, 1062 (8th Cir. 1982)).

[370] *See id.* at 689, 696-97.

[371] *See supra* note 31.

or other standard form clauses to the consumer's disadvantage in the U.S. and in Europe. Partly due to these issues the probability of the plaintiff prevailing in court will generally be substantially lower than one.

Finally, the international nature of many online transactions leads to yet another problem in regard to enforcing consumer rights in the courts. Should the consumer obtain a favorable judgment, this judgement eventually needs to be recognized and enforced in another jurisdiction. This is, of course, not necessary when the defendant has assets in the jurisdiction in which the judgment was entered. In the online environment, however, it has become much easier to engage in worldwide business without necessarily holding valuable assets abroad.[372] Consequently, if the consumer had the advantage of litigating in her home country (with the court possibly entering a default judgment in her favor) she often has the disadvantage of having to have the judgment recognized and enforced abroad—a timely, costly and often uncertain undertaking which always contains the risk that the judgment is held unenforceable[373] in the jurisdiction

---

[372] *See also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985). In this decision the Supreme Court already observed that "it is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted."

[373] *See generally* UNIF. FOREIGN MONEY-JUDGMENTS RECOGNITION ACT § 4 (1962); RESTATEMENT (SECOND) CONFLICT OF LAWS §§ 92, 98 (1971); GARY B. BORN, INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS 935 (3d ed. 1996) (all listing the grounds for non-recognition of foreign judgments in the U.S.). The historical basis for recognition of foreign judgments in the U.S. was laid down in Hilton v. Guyot, 159 U.S. 113 (1895).

Without going into further detail herein (for a more detailed discussion see Rufus Pichler, *Business-to-Consumer Electronic Commerce: The Economics of Litigation and Online Dispute Resolution* C. (Dec. 21, 1999) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies)), two particular prerequisites for recognition of judgments that exist in almost every jurisdiction should be pointed out: The court entering the judgment must

where assets can be found.[374] The expected judgment therefore does not necessarily reflect the expected benefit for the plaintiff. If she gets a judgment in jurisdiction X but the plaintiff only has assets in jurisdiction Y where this judgment (including an eventual claim for cost reimbursement) is not enforceable, the plaintiff's actual benefit is zero.[375]

### *ββ) Costs*

Not only does consumer litigation promise only low benefits, it is in general also relatively costly.[376] In our context this problem is aggravated because cross-border litigation is even more costly. It involves traveling time and costs, the need to hire foreign counsel, a need for foreign assistance in taking evidence, and

---

have had personal jurisdiction over the defendant according to the rules on jurisdiction of the recognizing state. And the defendant must have been served process in an appropriate manner (*see, e.g.*, Ackermann v. Levine, 788 F.2d 830, 837-38 (2d Cir. 1986)). Regarding the former it should be noted that in practice the vast majority of online merchants' terms of use will include choice of forum clauses establishing exclusive jurisdiction of the courts at the merchant's principal place of business. These clauses presently are generally not enforceable in Europe whereas U.S. courts are very likely to uphold them (*see* Pichler, *supra* at II.A.4.). European courts, for example, therefore would not be hindered by an online choice of forum clause to assert jurisdiction on general grounds such as local assets, affiliation, or consumer's place of residence (*see* Pichler, *supra* at A for a detailed discussion of international jurisdiction in regard to online transactions). In the context of recognition of judgments, however, the different attitudes regarding the enforceability of these clauses become decisively significant. Since U.S. courts, for example, honor the clause (leading to *exclusive* jurisdiction here) a European court's assertion of jurisdiction is necessarily inconsistent with American law. This means that a European judgment that was entered despite the existence of a clause establishing exclusive jurisdiction of U.S. courts, cannot be recognized and thus not enforced in the U.S.

[374] And of course fraudsters can deliberately hide their assets or locate them in jurisdictions known not to enforce foreign judgments.

[375] Hereinafter the benefit will be referred to as B. It is assumed that B = J in the case of an enforceable judgment and B = 0 in the case of an unenforceable judgment.

[376] This has been recognized long ago and led to an intensive discussion on "access to justice". *See generally* Posner, *supra* note 353, at 439-441. *See also* Rubin, *supra* note 214, at 119 ("[The] costs will often be sufficiently large to overwhelm any benefit from judicial enforcement. This will *almost always be the case for consumers*, ....") (emphasis added).

possible language barriers that may require costly translations of documents.[377] Given the low stakes involved it can be assumed that the litigation costs exceed the expected judgment in the majority of cases, even under the assumption that the probability of the consumer winning in court is one.[378] This alone, however, does not necessarily lead to a negative-expected value suit, because it depends on the applicable cost allocation system, whether the consumer actually has to bear her litigation costs or whether she is entitled to their reimbursement by the losing party.[379] Courts always apply the cost allocation system of the forum.[380] For this reason, the decision where to bring suit is also a decision for or against a specific cost allocation system.

In general, under the American rule, each party has to bear its own litigation costs. The British and continental system, however, requires the losing party to reimburse the winning party's litigation expenses.[381] Thus, the plaintiff will bring suit under the American system when her expected judgment exceeds *her*

---

[377] *See, e.g.*, BORN, *supra* note 373, at 5.

[378] It has been noted above that this is an unrealistic assumption, *see supra* text following note 358.

[379] *See* Shavell, *Suit, Settlement, and Trial, supra* note 353, at 56 (stressing the importance of the method of cost allocation). *See also*, Posner, *supra* note 353, at 428 *passim* (discussing the implications of different cost rules). *See generally* Philipp J. Mause, *Winner Takes All: A Re-Examination of the Indemnity System*, 55 IOWA L. REV. 26 (1969) (discussing the American and the British cost allocation systems).

[380] *See, e.g.*,

[381] At this point it is assumed that the winning party's expenses are fully reimbursed. In fact most systems provide some kind of absolute limitation and generally do not reimburse excessive costs. *See e.g.* § 91(1) ZPO (German civil procedure statute) (stating that the opponent's expenses are only to be reimbursed to the extent that they were "necessary"). *See also infra* note 396.

litigation costs,[382] and under the British and continental system when her expected judgment exceeds the expected litigation costs, being the sum of the plaintiff's and the defendant's costs multiplied by the probability of the plaintiff losing the case.[383] Therefore, even when the plaintiff would win her case for sure, she would not bring suit under the American cost allocation rule if her costs exceed the judgment.[384] This poses the known "problem of the meritorious small claim defeated by the litigation-expense threshold".[385]

*β) "The Consumer's Dilemma"*

Assume, for example, that a European consumer is thinking of bringing a claim against an U.S. merchant who has no assets in Europe. This leads to the following dilemma for the consumer who seeks judicial redress:

The consumer would normally chose to bring suit in Europe because under the European cost allocation system the losing merchant would have to reimburse the consumer's litigation costs and the expected judgment is greater than zero. However, since her expected judgment will most likely not be enforceable in the U.S.,[386] the consumer's expected benefit as well as the expected actual

---

[382] If $c_p$ are the plaintiff's costs and $c_d$ the defendant's costs (Court fees are assumed to be part of the plaintiff's costs) then suit will be brought if $pJ > c_p$.

[383] $pJ > (1 – p)(c_p + c_d)$ or, if the plaintiff's and the defendant's costs are assumed to be equal: $pJ > 2c – 2pc$. *See* Posner, *supra* note 353, at 437.

[384] This problem theoretically does not arise under the British and continental cost allocation rule. In reality, however, the problem is not solved, *see infra* note 390 and accompanying text.

[385] *See* Posner, *supra* note 353, at 438. *See also* Bebchuk & Chang, *supra* note 353, at 373 (suggesting alternative fee shifting rules taking into account the "margin of victory" to solve this problem).

[386] Assuming an exclusive forum selection clause in favor of a U.S. forum, *see supra* note 373.

reimbursement of her costs will be zero. The lack of enforcement turns it into a negative-expected value suit, the consumer gains nothing and loses her litigation expenses, and thus she will not bring suit in Europe.

The actual expected benefit is only positive when the consumer brings suit in the U.S. where the local judgment is per se enforceable. In the U.S., however, the consumer will have to bear her own litigation costs, which will typically exceed the expected judgment. Thus, the consumer will not bring suit in the U.S. either. She will, as a result, never bring suit.[387]

The above analysis suggests a different outcome, when a suit can be brought under the European cost allocation system and the plaintiff faces no uncertainty as to the expected judgment's enforceability. This would for instance be true if a U.S. consumer sued a European merchant in Europe, if a European consumer sued a merchant from another European country in her home courts,[388] or if a European judgment would be enforceable in the jurisdiction in which assets are located.[389]

---

[387] *See also* Muris, *supra* note 241, at 105 ("As is well known, however, for consumer transactions going to court is usually not economically feasible. When disputes involve small losses to consumers, private lawsuits will not work.").

[388] Art. 26 of the Brussels Convention guarantees recognition and enforcement of judgments from a signatory state in any other signatory state.

[389] E.g., in the unlikely case of the absence of a choice of forum clause. Another case would be one in which the defendant had sufficient assets in the jurisdiction rendering the judgment.

It is admittedly not as clear as before, but is also very unlikely that the consumer will actually bring suit in these cases.[390] The reasons, however, are different since under the same conditions as above the expected benefits would actually exceed the expected costs (being zero after reimbursement).[391] The first reason why even under the European rule small claims will still be defeated by costs is that the probability of winning is generally not one.[392] But even if it is only slightly less, the costs may quickly exceed the expected judgment.[393] Under the European rule the risk for the plaintiff actually becomes greater, because if she loses she will not only have to pay her own costs but her opponents' as well.[394]

Another reason why small claims won't be brought under the European cost allocation rule either is that even the successful plaintiff will not get a full reimbursement of her costs. This is generally true in the sense that she must always bear the opportunity costs of time spent during the litigation process.[395] Apart of that it is true when American plaintiff's bring suit in Europe, because of a substantial uncertainty as to what extent the generally much higher lawyer fees of an American lawyer will be held reimbursable by, for example., a German

---

[390] *See* Posner, *supra* note 353, at 438 (answering to the suggestion that "if the English practice of reimbursing the winning party's attorney and witness fees were adopted in this country, the problem of the meritorious small claim defeated by the litigation-expense threshold would be solved. It would not be solved.").

[391] Remember that in the case of enforceability of the judgment B = J and that the condition to bring suit under the European rule was J > 0 if p = 1.

[392] *See supra* text following note 358.

[393] *See* Posner, *supra* note 353, at 439 (giving the example the if p = .99 the stakes must be larger than one fiftieth of the litigation expense for the plaintiff to bring suit).

[394] *Cf.* Posner, *supra* note 353, at 428.

court.[396] This theoretical analysis, which suggests that even under the European cost allocation rule small claims are particularly unlikely to be brought if they require suing or enforcing a judgment in another jurisdiction, is backed by existing empirical studies.[397] In short it can be concluded that even in the cases introduced above, the consumer will hardly ever litigate a claim against a foreign merchant and cannot credibly threaten the merchant to do so in order to extract a settlement.[398] Consequently, individual court enforcement is no viable basis for consumer reliance.

### *bb) Rights to Sue for Consumer Organizations*

The problem of judicial redress or access to justice for consumers, whose meritorious small claims are defeated by high litigation costs, is not unfamiliar. It is an issue frequently addressed by the European Commission in its efforts to

---

[395] *See* Posner, *supra* note 353, at 438 ("The most important exclusion is the opportunity cost of the party's time, ...."); Landes, *supra* note 353, at 102 (costs from trial delay).

[396] *See* HAIMO SCHACK, INTERNATIONALES ZIVILVERFAHRENSRECHT para. 580d (2d ed. 1996). *See generally* Dieter Leipold, *Limiting Costs for Better Access to Justice: The German Approach*, *in* REFORM OF CIVIL PROCEDURE 265, 266-275 (A.A.S. Zuckermann & Ross Cranston eds., 1995); Bundesrechtsanwaltskammer [German Bar Association], *German Attorney's Fees* (visited Aug. 17, 00) <http://www.brak.de/aktuelles/3Dgebo-e.html> (explaining the German cost allocation system and its statutory lawyer fees).

[397] *See* BIRGIT FELDTMANN ET AL., THE COST OF LEGAL OBSTACLES TO THE DISADVANTAGE OF CONSUMERS IN THE SINGLE MARKET, A REPORT FOR THE EUROPEAN COMMISSION DG XXIV – CONSUMER POLICY AND CONSUMER HEALTH PROTECTION 277 (1998) (finding that since "costs in all member states soon exceed the value of the claim for all amounts of claim below 2,000 ECU, consumers are effectively barred from seeking redress for their most common problems.") (footnote omitted).

[398] The defendant will not agree to settle unless the plaintiff has a credible threat to sue or to proceed to trial (and assuming that plaintiff and defendant have common knowledge about the stakes and the costs). *See* Shavell, *Suit, Settlement, and Trial, supra* note 353, at 56 n.7; Shavell, *Incentive to Bring Suit*, *supra* note 353, at 338 (suggesting that absent a credible threat to sue the plaintiff won't even press a claim against the defendant); Cooter & Rubinfeld, *supra* note 353, at 1083; Posner, *supra* note 353, at 439.

enhance effective consumer protection.[399] A recent development in this field is granting consumer organizations a right to sue in the event of the violation of specific consumer protection laws.

The most relevant directive in our context, the Distance Contracts Directive,[400] for example, provides that "Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive in the interests of consumers." To understand the scope and significance of this provision one has to differentiate between two possible types of violation of the Directive's provisions: violations harmful to the *collective interests* of consumers and violations harmful to *individual interests* of a consumer. The first basically include non-compliance with the Directive's obligations to provide the required information,[401] a use of one of the prohibited aggressive marketing methods,[402] or a use of certain means of distance communication without the consumer's prior consent or despite her clear objection.[403] The latter include individual rights of consumers, namely the obligation of the supplier to *reimburse* the sums paid by the consumer when she exercises the right of withdrawal granted by the

---

[399] *See generally* European Commission, Health and Consumer Protection, *Access to Justice* (visited Aug. 17, 00) <http://www.europa.eu.int/comm/dg24/policy/developments/acce_just/index_en.html>. *See also* OECD, *Consumer Protection Guidelines, supra* note 142, at 7 (calling for a framework that "provides consumers with meaningful access to fair and timely dispute resolution and redress without undue cost or burden").

[400] *See supra* note 24.

[401] *See id.* arts. 4, 5.

[402] *See id.* art 9.

[403] *See id.* art 10.

Directive[404] and the right to be *recredited* with the sums paid in the event of a fraudulent use of her credit card.[405]

The remedies and means of judicial redress that are available in each of these cases vary, and it will be shown that the problem of consumer access to justice is not eased with regard to individual interests.

*α) Collective Interests of Consumers*

Referring to the "adequate and effective means ... to ensure compliance with this Directive" art. 11(2) states that these "shall include" a right for public bodies, consumer organizations, and/or professional organizations to take action before courts or competent administrative bodies to ensure that the national provisions for the implementation of the Directive are applied.

Although art. 11(1) would by itself not necessarily exclude individual consumer interests from its scope, it has been interpreted as to only refer to collective consumer interests.[406] This is consistent with the Directive on Injunctions for the Protection of Consumer's Interests.[407] This Directive aims at an approximation of the laws of the Member States relating to actions for injunctions aimed at the

---

[404] *See id.* art. 6(2).

[405] *See id*. art. 8.

[406] *See* BMJ, *Draft Distance Contracts Act, supra* note 69, at 64 (stating that the right of the aforementioned entities to bring an action was meant to facilitate monitoring of general business practices, but cannot have been meant to enable these entities to enforce contractual claims of individual consumers). *See also supra* note 239 and accompanying text.

[407] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on Injunctions for the Protection of Consumer's Interests, 1998 O.J. (L 166) 51. The Directive

protection of the collective interests of consumers.[408] It explicitly excludes individual consumer interests and the "cumulation of interests of individuals who have been harmed by an infringement."[409]

Any "infringement", i.e. any act contrary to the Directives listed in the Annex[410] (including the Distance Contracts Directive), which harms the collective interests of consumers,[411] may be challenged in the courts by qualified public bodies or organizations whose purpose it is to protect such interests.[412] The actions are viewed as tort actions (for an infringement of the listed Directive's provisions) rather than contract actions, which is relevant to determine the applicable law and the competent courts. Applying the general rules for tort actions, both the courts of the Member State where the infringement originated or, more relevant with regard to foreign merchants, the courts of the Member State where the infringement has effects can assert personal jurisdiction.[413] The effect of the infringement will generally occur in all states in which consumers are affected by

---

entered into force on July 1, 1998 and will have to be implemented within 30 months from this date, *see id.* arts. 8, 9.

[408] *See id*. art 1(1).

[409] *See id*. recitals para. 2. The Directive thus does *not* introduce class actions. Class actions (in the U.S.), by the way, have not proven feasible to address the problem of access to justice either, *see, e.g.*, Muris, *supra* note 241, at 105 ("Nor have class actions evolved to provide adequate enforcement [regarding disputes that involve small losses for consumers].").

[410] These are all Directives related to consumer protection.

[411] *See id.* art. 1(2) (defining "infringement").

[412] *See id.* arts. 2, 3 (defining and specifying the type of actions that can be brought and the entities qualified to bring them).

[413] The same rule applies to determine the applicable law. *See* Directive 98/27/EC, *supra* note 401, art. 2(2) (referring to this general rule of private international law). *See also id.* recitals para. 6.

the business practices of the merchant, i.e. all states where that merchant conducts business.

In sum foreign merchants might have to fear actions for infringement of collective consumer interests brought in European courts by specific public bodies or private organizations. The remedy will normally be an injunction requiring the cessation of the infringement accompanied by an obligation to make payments into the public purse or to nationally designated beneficiaries in the event of failure to comply with the decisions.[414] The threat to bring these actions is generally quite powerful taking into account the much better financial equipment of these entities as compared to individual consumers. And if the merchant has any assets in Europe she also faces actual enforcement of the decisions. If it does not have any assets in Europe, however, the practical risk may be considerably lower due to the uncertainty regarding recognition and enforcement of the respective actions in the country where that merchant has assets.[415]

*β) Individual Interests of Consumers*

As indicated above, however, the right of qualified entities to bring an action does not cover claims of individual consumers. It does not include the claim for reimbursement of the sums paid by a consumer that arises after exercising the right of withdrawal, or any other claim arising from breach of contract or fraud. Regarding consumer reliance, the right therefore faces the same limits like

---

[414] *See id.* art. 2(1).

[415] *See supra* note 373.

criminal enforcement actions.[416] Consumer redress is not facilitated. Consequently, the right of certain organizations to protect collective interests of consumers—just as criminal proceedings—does not provide a means on which potential online customers can or will rely to "fix things if they go wrong."

### c) Organization Enforcement and Codes of Conduct (Self-Regulation)

Ever since the Internet and electronic commerce have drawn increased attention of policymakers and businesses, "self-regulation" has been a hot topic. Initially the discussion—mainly in the abundant law journal literature—was polarized. On the one side stood a somewhat idealistic cyber-libertarian conception of the Internet as a stateless "place", in which online communities develop a comprehensive system of self-governance[417] without any state's interference.[418]

---

[416] *See supra* text following note 347.

[417] *See* David R. Johnson & David Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). *See also* David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art 3 (June 1995) <http://warthog.cc.wm.edu/law/publications/jol/post.html> ; David G. Post, *The "Unsettled Paradox": The Internet, The State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521 (1998); David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155 (1996); David G. Post & David R. Johnson, Working Paper, *The New Civic Virtue of the Net: Lessons from Models of Complex Systems for the Governance of Cyberspace*, 1997 STAN. TECH. L. REV. (visited Aug. 17, 00) <http://stlr.stanford.edu/STLR/Working_Papers/97_Post_1/index.htm>; John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT. L.J. 207, 224 (1997); Amy Knoll, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275, 301 (1996); Eric J. McCarthy, *Networking in Cyberspace: Electronic Defamation and the Potential for International Forum Shopping*, 16 U. PA. J. INT'L BUS. L. 527, 564 (1995). For an overview on the beginnings of the self-governance discussion see Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1665-1670 (1995).

[418] A famous account of this conception is given by John Perry Barlow, *A Cyberspace Independence Declaration* (Feb. 9, 1996) <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>:

„Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

On the other side stood those who feared "cyber-anarchy" and had no problem with government regulation, since the Internet should not be treated differently.[419] As, during the process of commercialization of the Net,[420] people more and more supplanted the term "cyberspace" with "e-commerce" an unlikely alliance formed: The idea of self-regulation was adopted by business, those "'immigrants' from the real world who are arriving in droves in the belief that cyberia's highways are paved with gold."[421] The alliance was unlikely because these were exactly those immigrants who threatened (and to the largest extent succeeded) to forever change the cyber-libertarian's social space into a mere global marketplace. Business very much liked the idea of running things on its own, adopting codes of conduct and other industry standards,[422] and trying to avoid government regulations which were feared to be too constraining for the development of

---

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. [...]."

[419] *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998), Jonathan D. Bick, *Why Should the Internet be Any Different?*, 19 PACE L. REV. 41 (1998). *See also* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1402 (1996); Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561 (1998).

[420] *See supra* note 9.

[421] Dunne, *supra* note 9.

[422] *See, e.g.*, Alliance for Global Business, *supra* note 17, at 8 (stating a number of fundamental principles that should shape the policies that govern electronic commerce, the first of which reads that "[t]he development of electronic commerce should be led primarily by the private sector in response to market forces", and the eighth of which argues that "[t]he protection of users ... should be pursued through ... industry-led solutions"); Global Business Dialogue on Electronic Commerce (GBDe), *supra* note 20, par. 5 ("develop effective self-regulatory and market-driven mechanisms"). *See generally* Rothchild, *supra* note 31, at 946-49 (giving an overview on basic tools of industry self-regulation).

electronic commerce.[423] On the other hand, government—at least in the U.S.[424]—never played the part of the tough adversary and initially propagated a leadership of the private sector as well.[425] Meanwhile, in the regulatory discussion, the artificial dichotomy of self-regulation versus government regulation has been replaced by more realistic thoughts about cooperation between the private and the public sector and on finding the right mix between the two.[426] In some areas, particularly pertaining to privacy, regulators more and

---

[423] Some argue that commerce acts together with government which regulates code, *see* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 43-62 (1999). *See also* Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703 (1998).

[424] The European Union wanted to establish a comprehensive regulatory framework from the very beginning, *see* A European Initiative in Electronic Commerce, COM(97)157 final at 12 ("The objective of the Commission is to implement the appropriate regulatory framework by the year 2000."), available online at <http://www.ispo.cec.be/ecommerce/legal/documents/com97-157/ecomcom.pdf>. *See also* David Church et al., *Recent Developments Regarding U.S. and EU Regulation of Electronic Commerce*, 33 INT'L LAW. 347, 347-355 (1999). *But see* Matthew J. Feeley, *EU Internet Regulation Policy: The Rise of Self-Regulation*, 22 B.C. INT'L & COMP. L. REV. 159 (1999) (detecting a policy shift towards supporting industry self-regulation as a reaction to the release of President Clinton's framework).

[425] *See* FRAMEWORK, *supra* note 15, at 1. ("[G]overnments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet."). *See also* WORKING GROUP I, *supra* note 4, at 5 (emphasizing private sector leadership and reliance on market forces instead of government regulation), at 8 ("privately enforced codes of conduct should be a central instrument"); WORKING GROUP II, *supra* note 4, at 10, 17 (promoting private sector leadership and the development of effective codes of conduct).

[426] *See* OECD, Directorate for Science, Technology and Industry, *OECD Forum on Electronic Commerce: Report on the Forum*, SG/EC(99)12 at 13 (Nov. 24, 1999), available online at <http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/forum_report.pdf> (reporting the concluding remarks by Mr. Herwig Schlögl, saying that "[p]eople no longer speak of a dichotomy [regarding the issue of regulation and self-regulation]—rather the challenge is to get the mix between these complementary approaches right"); Alliance for Global Business, *supra* note 17, at 10 ("It is important to recognise the need for global cooperation by both business and governments to facilitate electronic commerce.") (*but see infra* note 430); Ernest T. Patrickis & Stephanie Heller, *The Government's Role in Electronic Commerce: A Review of the Clinton Administration's Framework on Global Electronic Commerce*, 18 ANN. REV. BANKING L. 325, 326 (1999) (discussing the government's role in *supporting* business and commerce as laid out in the framework). *See also* Llewellyin Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 509, 523 (1997); Dunne, *supra* note 9, at 11; Henry H. Perritt, Jr.,

more start to express doubts, whether self-regulation is still a promising approach.[427] And, without having to decide in general which approach or which mix is best suited from a regulatory or *public policy* point of view, doubts are also appropriate as to whether self-regulation is capable of establishing consumer confidence—meaning as to whether consumers, from their *individual* point of view, are likely to *rely* on self-regulatory mechanisms.[428]

Business alliances, however, keep propagating that industry self-regulation and codes of conduct[429] should be favored wherever and to the largest extent

---

*Townhall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413, 433 (1997) (all arguing for self-regulation on a *contractual* basis in the limits of government regulation); Todd H. Flaming, *The Rules of Cyberspace: Informal Law in a New Jurisdiction*, 85 ILL. B.J. 174, 179 (1997) (arguing for self-regulation only pertaining to "internal problems"); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 926 (1996) ("For global networks, governance should be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behavior will come from each of these interest centers."); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 995, 1025 (1994) (proposing a step-by-step system from "bottom up" to „top down" regulation, starting with pure self-help and going to contract approaches and ultimately government regulation); Rothchild, *supra* note 31, at 968 (government regulation should support and complement the private sector).

[427] *See, e.g.*, Robert Pitofsky, *Electronic Commerce and Beyond: Challenges of the New Digital Age* (Feb. 10, 2000) <http://www.ftc.gov/speeches/pitofsky/rpwilson2.htm> ("To date, much of the online debate has centered around several options -- do nothing to protect consumer privacy ("hands off the Internet"), industry self-regulation, or government regulation. Given the invasions of privacy that we have seen in the early stages of development of online commerce - some involving the illegal collection of personal information from kids - and the constant concern by online participants about invasions of their privacy, the do-nothing option does not seem appealing.") (footnote omitted). Privacy advocates like the Electronic Privacy Information Center (EPIC) agree and also call for enforceable *legal* protection, *see* Sarah Andrews & Andrew Shen, Electronic Privacy Information Center, *Public Comment on Barriers to Electronic Commerce: U.S. Department of Commerce—Office of the General Counsel; Laws or Regulations Posing Barriers to Electronic Commerce* (Mar. 17, 2000) <http://www.epic.org/privacy/internet/Barriers_to_E-commerce.html>.

[428] *See infra* II.C.1)c)bb).

[429] For an example of a code of conduct see BBBOnline, *Code of Online Business Practices* (visited Aug. 17, 00) <http://www.bbbonline.com/businesses/code/index.htm>. *See also* OECD, *Consumer Protection Guidelines, supra* note 142.

possible.[430] And they can, in fact, point to some well-known historic examples of successful industry self-regulation.[431]

### *aa) Historic Examples of Successful Industry Self-Regulation*

A number of "classic" studies of merchant and industry self-regulation and of informal enforcement mechanisms suggest the suitability of these mechanisms to ensure desired behavior within a specific group of agents under specific circumstances. These studies include[432] more recent phenomena such as Bernstein's analysis of extralegal contractual relations in the diamond industry,[433] as well as self-regulation in the pre-industrial era such as enforcement

---

[430] *See* Alliance for Global Business, *supra* note 17, at 6 ("The pace of change and nascent state of electronic commerce have heightened the risks associated with premature or unnecessary government regulation. This has increased the responsibility of business to promote a trustworthy environment through self-regulation and technological innovation. Business has a strong market incentive to foster the empowerment of users, but will only make the necessary investments if it can trust that governments will *recognise and reinforce the leadership of business in responding to the highly dynamic nature of electronic commerce*.") (emphasis added); Global Business Dialogue on Electronic Commerce (GBDe), *supra* note 20, par. 7 ("[W]e give precedence to effective self-regulation and technological solutions wherever possible ... any intervention of public authorities should be narrowly tailored, ....").

[431] And implicitly they do, *see* Alliance for Global Business, *supra* note 17, at 6 ("Self-regulation is not a new phenomenon. Throughout history, business has set its own standard rules and practices through a variety of organisations to lower transaction costs, to avoid and resolve conflicts, and to create consumer confidence.").

[432] For a general overview see, for example, Lisa Bernstein, *Private Commercial Law, in* 3 THE NEW PALGRAVE, *supra* note 149, at 108; Avner Greif, *Institutions and International Trade: Lessons from the Commercial Revolution*, 82 AEA PAPERS & PROC. 128 (1992) [hereinafter Greif, *Commercial Revolution*]; Avner Greif, *Informal Contract Enforcement, in* 2 THE NEW PALGRAVE, *supra* note 149, at 287 [hereinafter Greif, *Contract Enforcement*].

[433] *See* Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. LEGAL STUD. 115 (1992).

mechanisms at medieval champagne fairs,[434] the coalition of Maghribi traders in the 11th century,[435] or the merchant guilds.[436]

The diamond industry, to the largest extent, operates outside the formal legal system. It has developed its own internal business norms and customary practices, provides an exclusive arbitration system in cases of a breach of these rules, and has found effective ways to enforce its own rules "completely outside the legal system."[437] Similar mechanisms have evolved in other exchanges, the New York Stock Exchange—early in its history—being cited as a prominent example.[438] Exchanges created standardized systems of measuring the attributes of commodities, formulated rules of trade and acceptable or unacceptable behavior, imposed disclosure obligations, mediated disputes, and provided for contract enforcement by arbitration.[439] Less recent examples of self-regulation go back to a time characterized by the "absence of appropriate legal enforcement provided by the state."[440] Given this paper's preceding analysis of

---

[434] *See* Paul R. Milgrom et al., *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs*, 2 ECON. & POL. 1 (1990).

[435] *See* Avner Greif, *Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition*, 83 AM. ECON. REV. 525 (1993).

[436] *See* Avner Greif et al., *Coordination, Commitment, and Enforcement: The Case of the Merchant Guild*, 102 J. POL. ECON. 745 (1994).

[437] *See* Bernstein, *supra* note 433, at 138, 157.

[438] *See* Stephen Craig Pirrong, *Self-Regulation of Private Organized Markets, in* 3 THE NEW PALGRAVE, *supra* note 149, at 433, 434. Later, however, these exchanges more and more became subject to government-regulation, *see id.* at 437 ("Governments have largely supplanted exchanges in several crucial areas of regulation.").

[439] *See id.* at 434.

[440] *See* Greif, *Contract Enforcement, supra* note 432, at 288. The historic background is the re-emergence of long-distance trade in Europe and the Mediterranean region in the eleventh to fourteenth century.

the role and effectiveness of state enforcement in the online context, the current situation seems quite comparable.[441] While common state rules where lacking, merchants created their own norms of trade, namely the *law merchant*, which was applied by private judges, often merchants themselves.[442] But the Law Merchant system was eventually replaced by a "system of state enforcement ..., especially in later periods when nation states exercised extensive geographic control."[443] When, however, as in the current period of globalization, nation states' geographic control arguably becomes increasingly toothless, it seems that an argument for a revival of the self-regulatory *lex mercatoria* (in the form of a *lex informatica*) could be made.[444] Another example of successful self-regulation in the late middle ages is the merchant guild, which successfully ensured "the coordination and internal enforcement [of its norms and regulations]" needed to permit effective collective action.[445]

---

[441] Even more so, when one notes that one of the main reasons for the lack of state enforcement then—as today—are "the boundaries of the state's jurisdictional power" and the resulting "absence of ... authority over (all) those parties to the exchange who can gain from breaching the contract." *See id.* at 287.

[442] *See, e.g.*, Milgrom et al., *supra* note 434, at 2, 4-6.

[443] *See id.* at 20.

[444] In fact, of course, it is made. *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998). *See also* Robert D. Cooter, *Structural Adjudication and the New Law Merchant: A Model of Decentralized Law*, 14 INT'L REV. L. & ECON. 215, 216 (1994) (referring to rules and norms within modern business communities as the new law merchant).

[445] *See* Greif et al., *supra* note 436, at 748. The collective action was the coordinated response by a large fraction of merchants in the form of a boycott, when a ruler did not provide some of them the necessary protection, *see id.* at 753. In our context the fact that the internal norms to act in a specific way (boycott) were successfully enforced is the important part.

### *bb) It's a Different World Online—The Failure of Self-Regulation as a Basis for Consumer Reliance*

These examples show that self-regulation may work—under specific conditions. These conditions, however, are the important part, and they are not met in the online world.

In some of the examples, self-regulation was limited to *internal* relations, to acts that have effects only within the regulatory group or association. The Law Merchant, for example, regulated trade *between merchants* rather than establishing rules for retail to non-merchants. Also, in the diamond industry, the trading norms, dispute resolution and enforcement mechanisms are only employed in dealings between dealers that are members of the bourse.[446] Agreements involving the rights of third parties do not fall within the industry's extralegal regime.[447] This, however, is not a necessity. It may very well be in the interest of the self-regulating group to address behavior of members that will have *external effects* because these effects can backfire and have negative consequences for the group as a whole. Early exchanges, for example, articulated rules against fraud of external investors by members of the exchange,[448] presumably because all the exchange members were at risk of losing their credibility if one of them engaged in such behavior. A similar *external*

---

[446] *See* Bernstein, *supra* note 433, at 152 (saying that *nonmembers* might behave in a certain way not to hurt their chances of joining the bourse, but not speaking of any incentives for members to do so, when they deal with nonmembers).

[447] *See id.* at 154.

[448] *See* Pirrong, *supra* note 438, at 435 ("Exchanges have also devised means of protecting investors against fraud and the consequences of default by brokers.").

regulation existed in the merchant guild. Members of the guild were forced to take part in the boycott of a nonmember—a ruler or city that did not afford one or a few of the guild members the necessary protection.[449] Propagated self-regulation of online merchants would operate in a comparable manner. Online merchants would agree to specific codes of conduct pertaining to behavior towards consumers, i.e. behavior with *external* effects. Thus, in this regard online self-regulation is not significantly different from some forms of successful self-regulation discussed above. The difference between a purely *internal* and an *external* self-regulation, however, is noteworthy nevertheless. When relating to externalities, self-regulation has frequently turned out to be less viable and to a large extent to be supplanted by government regulation.[450]

However, the key difference between the successful examples of self-regulation discussed above and the propagated self-regulation of online merchants—which, for exactly this difference, will not be successful—is another. It is the *lack of internal enforceability* in the online world. In each of the examples discussed above, self-regulation was successful because the regulating group or association had the power to enforce its norms against its members and coerce them to comply with them. The group could credibly threaten to impose sanctions

---

[449] *See* Greif et al., *supra* note 436, at 752 ("In each case, merchants imposed a collective punishment on the city that included participation by merchants who had not been directly injured.").

[450] *See* Pirrong, *supra* note 438, at 437 (pointing to commodity exchanges and future trading, where "current law does not rely exclusively upon self-regulation to reduce the frequency of manipulation and fraud"); Bernstein, *supra* note 432, at 114 (pointing to asymmetries in information and unequal bargaining power that can give rise to questioning the legitimacy of *private commercial law*).

on potential deviators that were severe enough to make them play by the rules from the outset most of the times. Greif, for example, notes that for the merchant guild to be successful it was crucial that it was an "organization with the ability both to coordinate ... decisions and to *enforce* them by applying sanctions on its own members."[451] In the context of the guilds these sanctions consisted primarily of excluding a member from important trading places or expelling them from the guild altogether.[452] In other contexts, too, merchants were induced to behave honestly by the threat of being boycotted or ostracized.[453] Similarly, diamond trading clubs would impose fines on members who did not honor the internal norms or ultimately expel them from the trading club,[454] and exchanges would suspend or expel members under similar circumstances.[455]

The value of the membership to the member (or the cost of losing it) is a crucial factor for expulsion to be a credible threat. Since membership in each of these groups is voluntary to begin with, merchants cannot literally be *compelled* to obey a rule. They could always leave or withdraw.[456] The viability of the whole system of organization enforcement thus depends on whether the benefits of group membership exceed the costs of obeying the group's norms (or the benefits of

---

[451] *See* Greif et al., *supra* note 436, at 753.

[452] *See id.* at 757, 760.

[453] *See* Milgrom et al., *supra* note 434, at 3, 6. As a second step, "a merchant who fails to deliver a punishment, say by participating in a boycott, when he is supposed to do so is himself subject to punishment by the community of merchants." *See id.* at 8.

[454] *See* Bernstein, *supra* note 433, at 120, 129.

[455] *See* Pirrong, *supra* note 438, at 434.

breaking them).[457] In the "classic" examples discussed above, this was clearly the case. A diamond dealer, who does not have access to the trading clubs, will be at a competitive disadvantage.[458] In fact, "[b]eing subject to these types of sanctions [suspension, expulsion] makes it unlikely that a trader will be able to remain in the diamond business" at all.[459] The fact that club membership is essential to maintaining a viable business gives the club a strong leverage to actually force members to comply with the self-regulatory regime. Similarly, exclusion of a medieval merchant from the guild and the trading places, protection, and economic rent it provided[460] or from important trade fairs,[461] was likely to mean the end of that merchant's business.

In the online context, however, these conditions are not met. While a high degree of interdependency among merchants is needed to make threats of boycott or expulsion credible, electronic commerce is, to the contrary, characterized by its high degree of *autonomy*. People can be authors and publishers of their works, and merchants can be manufacturers, marketers, and distributors of their products or services at the same time.[462] Online "anyone with a laptop and a

---

[456] *See id.* at 436 (stating that "the voluntary nature of an exchange limits its coercive power" and that a member cannot literally be comp

[457] *See also id* at 436; Bernstein, *supra* note 432, at 109 ("the effectiveness of these sanctions varies and is closely linked to the value of association membership").

[458] *See* Bernstein, *supra* note 433, at 119.

[459] Bernstein, *supra* note 432, at 109.

[460] *See* Greif, *Contract Enforcement, supra* note 432, at 289; Greif et al., *supra* note 436, at 758.

[461] *See* Milgrom et al., *supra* note 434, at 20.

[462] *See also* Heckman, *supra* note 113, at 1.2 ("Many vendors can sell globally without the costly infrastructure of world-wide retail stores, sales offices, distributors, or warehouses.").

modem can open a storefront and have access to a global marketplace."[463] The dependency on suppliers, distributors, trading partners, or entrance to physical trading places diminishes,[464] and consequently the leverage of industry groups or trade associations does, too. While this is clearly the case in regard to merchants providing services or information, which can be *self-generated*, it seems less clear in regard to tangible products. These still have to be produced and delivered which arguably would put manufacturers and distributors in a position to impose sanctions on fraudulent merchants. In theory this is true. The problem with fraudulent merchants, however, is that they typically *neither have, nor deliver* the goods they are selling to consumers.[465]

When the U.S. Government's Working Group on Electronic Commerce asserts that "[s]elf-regulation in the digital age will require the private sector to engage in much greater collective action to set and enforce rules than was characteristic of the Industrial Age",[466] we face a dilemma. The very nature of electronic commerce and the increasing *autonomy* of agents in this field makes it much more difficult if not impossible for the private sector to engage in such collective action and to *enforce* rules than it was in the Industrial age, which was characterized by a much higher degree of dependencies and interdependencies.

---

[463] WORKING GROUP II, *supra* note 4, at v.

[464] *See also* OECD, *Business-to-Consumer Electronic Commerce: Survey of Status and Issues*, OCDE/GD(97)219, at 39 <http://www.oecd.org/dsti/sti/it/ec/prod/gd97219e.pdf> ("Today, it is no longer necessary to have stocks, means of transportation, warehouses, or money collection systems."). Why means of transportation or money collection systems are assumed to no longer be necessary remains unexplained, however.

[465] *See supra* note 112 and accompanying text.

Absent a credible threat of internal enforcement, industry self-regulation remains voluntary. Self-regulation, as it has been put, "only binds the 'good guys'."[467] Then, however, it *cannot be a basis for consumer reliance*. If industry norms, for example obligating merchants to refund consumers, cannot be enforced, a consumer cannot be confident that things can be fixed should they go wrong. Industry norms under these conditions only make sense as long as they are complied with. When a consumer has been defrauded, they are of no use, because they cannot effectively ensure consumer redress. This is not to say that industry self-regulation is useless altogether. Although the norms don't provide *enforcement* and therefore are no basis for consumer *reliance*, the fact that they may be adhered to by "the good guys" might become relevant in the context of *compliance* and *trust*.[468]

### d) Informal Enforcement of Social Norms

For similar reasons, social norms will not provide an effective enforcement mechanism in the online context either. This would require the existence of a close-knit, interdependent, and to a great extent homogenous community.[469]

---

[466] *See* WORKING GROUP I, *supra* note 4, at 8.

[467] *See* Rothchild, *supra* note 31, at 964 n.291 (citing Angela Drolte, *U.S. Consumers Advocate Doubts Effectiveness of Industry-Initiated Online Privacy Policies*, 2 ELECTRONIC COMMERCE & L. REP. (BNA) 601 (June 13, 1997) who quotes the testimony of Janlori Goldman at an FTC public workshop on consumer information privacy).

[468] *See infra* II.D.

[469] *See* ELLICKSON, *supra* note 213, at 177 ("[W]elfare-maximizing norms emerge in close-knit settings .... [A]n informal-control system may not be effective if the social conditions within a group do not provide members with information about norms and violations and also the power and *enforcement opportunities needed to establish norms*.") (footnote omitted) (emphasis added) and at 181 (defining a close-knit group "as a social network whose members have *credible and*

While such a group, consisting of technologically sophisticated experts with a common understanding and an unwritten code of behavior might have existed in the early stages of the Internet, it doesn't any more. With the commercialization of the net[470] the formerly homogenous group of *users* is split into *merchants* and *consumers*.[471] And even within each of these groups one is likely to find a heterogeneous structure of social, cultural, economic, moral, and criminal versatility and diversity. The times in which the majority of users were familiar with the behavioral norms of "netiquette"[472] are over.[473] Thus, even *identifying* commonly accepted social norms would most likely be impossible.[474] *Enforcing* them, due to the lack of interdependence and social ties within and among the

---

*reciprocal prospects for the application of power against one another* and a good supply of information on past and present internal events") (emphasis added). *See also* Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349, 359-60 (1993) ("Professor Ellickson and all the other commentators writing on this subject also recognize, however, that there are important preconditions for informal community governance without a major role for law. Most important among these is the likelihood of continuing relationships among the people making, enforcing and violating the rules and the existence of multidimensional relationships in the community.") (footnote omitted).

[470] *See supra* notes 9, 420.

[471] *Cf.* Gibbons, *supra* note 426, at 478 ("putative needs of the growing commercial sector of the Internet and the demands that it is making on governments is the greatest threat to the existing libertarian paradigm in Cyberspace").

[472] For a description of these norms see, for example, David E. Sorkin, *Revocation of an Internet Domain Name for Violations of "Netiquette": Contractual and Constitutional Implications*, 15 J. MARSHALL J. COMPUTER & INFO. L. 587, 597-99 (1997). Compilations of rules of netiquette can be found on numerous sites on the web. One of the most referred to seems to be Network Working Group, *Request for Comments: 1885—Netiquette Guidelines* (Oct. 1995) <http://www.ietf.org/rfc/rfc1855.txt>.

[473] *See also* Dunne, *supra* note 9, at 8 ("[t]his aspect of cyberian character seems slowly to be eroding"); FUKUYAMA, *supra* note 145, at 196 (stating that as the number of Internet users rose it included some "who did not feel bound by the ethical constraints of the original Internet community").

[474] *See also* Perritt, *supra* note 469, at 360 ("As the scope of networking increases, the likelihood that users will share values and feel membership to be essential decreases."). The breakdown of the consensus regarding the impermissibility of spamming (unsolicited commercial email), which

two groups, definitely is. Classic tools that the "cybercommunity" used to employ in response to behavior it disapproved of will hardly induce fraudulent merchants to change their behavior. This "social enforcement model"[475]—using flaming,[476] banishment,[477] disconnection,[478] or mailbombing[479]—will be increasingly ineffective because rule violators don't care, find alternative net access that is beyond the reach of the "enforcers",[480] or use technological protections.[481] Most importantly, however, none of these "enforcement" mechanisms is capable of redressing defrauded consumers. The reach of the internal enforcement tools of

---

meanwhile is obviously no longer regarded impermissible by a number of merchants, is just one example.

[475] *See* Perritt, *supra* note 469, at 355. *See also* Gibbons, *supra* note 426, at 510.

[476] The public expression of disapproval, *see, e.g.*, Gibbons, *supra* note 426, at 493-94.

[477] A sanction frequently employed in Multiuser Dungeons (MUD's). For a general description of MUD's see Pavel Curtis, *MUDding: Social Phenomena in Text-based Virtual Realities, in* HIGH NOON ON THE ELECTRONIC FRONTIER, *supra* note 9, at 347. The most famous example of such a banishment or toading (a virtual death penalty) is that of Mr. Bungle from the virtual community LambdaMoo (For a detailed description of Lambda Moo see Charles D. Siegal, *Rule Formation in Non-Hierarchical Systems*, 16 TEMP. ENVTL. L. & TECH. J. 173, 199-208 (1998)). Mr. Bungle was spoofing other characters of the community and engaged in "sexually explicit verbal rape" (Wells Branscomb, *supra* note 417, at 1662). For a description of this case see also Flaming, *supra* note 426, at 177; Gibbons, *supra* note 426, at 522; Rothchild, *supra* note 31, at 967; Julian Dibbell, *A Rape in Cyberspace; or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society, in* HIGH NOON ON THE ELECTRONIC FRONTIER, *supra* note 9, at 375.

[478] Also known as denial or termination of access. *See* Perritt, *supra* note 426, at 464; Perritt, *supra* note 469, at 356 ("disconnection enforcement model"); Reidenberg, *supra* note 426, at 920.

[479] *See* Wells Branscomb, *supra* note 417, at 1657-59; Flaming, *supra* note 426, at 176 (both describing the often cited case of the law firm Canter & Siegel whose server broke down as a consequence of masses of emails sent by users who disapproved of a previous spam by that firm).

[480] *See* Perritt, *supra* note 469, at 356 ("This simple remedy hides the fact, ..., that the user of network services is not really at the mercy of the rule setter, the supplier. If the user does not like the content of the rules, if the maker of the rules does not follow them or if the user is wrongfully disconnected, the user simply switches to another network. In a perfectly competitive market, this is not a problem for the user. It is as painless as calling one telephone number instead of another.").

[481] Spammers frequently use "dead" email addresses so that the returned mailbomb ends up in oblivion.

cyberspace is limited to assets in cyberspace—they cannot reach material assets or bank accounts in the real world. This latter limitation—regardless of whether social norms may (still) be identified in the online environment and of whether, if they can, online "enforcement" tools can effectively be employed—renders the social enforcement model completely unsuitable as a basis for *consumer reliance*. Consumers simply cannot have the confidence that the social enforcement model will fix things if they go wrong and compensate a consumer for an eventually incurred loss, because this model just can't do it.

### *2) Compliance*

The ineffectiveness of traditional enforcement mechanisms does, of course, not mean that every merchant behaves opportunistically all the time. Often, rational merchants will find it in their own interest to live up to agreements even though a third party could not effectively coerce them to do so. This is referred to herein as voluntary[482] *compliance*[483] and it is also frequently discussed under the heading of "self-enforcing contracts."[484] The economic mechanisms that lead to this kind

---

[482] Voluntary in the sense that no third party could actually *force* the merchant to comply. Voluntary does not mean, however, that a merchant does not *feel* compelled to comply out of economic considerations (namely because he fears non-legal sanctions).

[483] *See also supra* note 216.

[484] *See, e.g.*, Greif, *Contract Enforcement, supra* note 432, at 289 (describing the decisions of the merchant guilds and multilateral punishment of violators by the coalition of Maghribi traders as self-enforcing—due to the formers' ability to exclude and the latters' collective retaliation if only one of them was cheated).*See also* Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615, 636 (1981) ("non-third-party method of contract enforcement").

of self-enforcement are *non-legal sanctions*.[485] In our context two grounds for such sanctions (i.e. ceasing to transact in the future) are of particular interest: experience and reputation.[486] Both deal with reactions of potential future customers, but they are distinct in regard to the specific individual or group that imposes the non-legal sanction. Experience means the personal experience of only one specific customer with a particular merchant. This experience is the basis for her decision to transact with that merchant again. Reputation, on the other hand, depends on the dissemination of *information* about someone else's experience to other people that have not yet had any personal experience with that particular merchant and whose decision whether they will in the future obviously depends on whether the reputation is good or bad.

### a) Experience (Bilateral Reputation Mechanism)

Merchants who want to establish long-term relationships with their customers and would like them to engage in repeat dealings, are well advised to comply with their obligations—even in the absence of a credible enforcement threat. As Macaulay noted, you don't get many repeat orders from unhappy customers.[487]

---

[485] *See generally* David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373 (1990); Klein & Leffler, *supra* note 484; Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action*, 63 U. CHI. L. REV. 133 (1996).

[486] This distinction is also implicitly suggested by Macaulay, *supra* note 199, at 63-64 ("One is concerned with both the reaction of the other party in the *particular* exchange and with his own *general* business reputation. ... [S]ellers hope for repeat orders, and one gets few of these from unhappy customers. ... Not only do the particular business units in a given exchange want to deal with each other again, they also want to deal with other business units in the future.") (emphasis added). Others speak of a *bilateral* and a *multilateral* reputation mechanism (*see, e.g.*, Greif et al., *supra* note 436, at 748, 751), basically making the same distinction.

[487] *See* Macaulay, *supra* note 199, at 63.

The theory of repeated games points out, that, in an *iterated Prisoner's Dilemma*, an agent will not engage in further transactions with the same partner,[488] when her counterpart behaved opportunistically in the preceding game.[489] Because of this consequence a merchant who does not comply in game one might make a larger profit (i.e. get something for nothing)[490] in that round but risks to lose future income from potential repeated dealings with that customer. When the long-term benefits from repeated dealings exceed the short-run profit from defecting, the merchant has an incentive to cooperate and the contract becomes self-enforcing.[491] The relationship itself becomes a valuable asset and serves as a bond.[492] Note, however, that a merchant won't comply when the gain from dishonest behavior is larger than the expected future income:[493] "The committing party will breach whenever the benefits of breach out-weigh the cost of sacrificing the bond."[494] This may frequently be the case when a merchant who behaves

---

[488] Trading with the same partner, or "clientization," is central to *bilateral* reputation mechanisms. *See, e.g.*, Milgrom et al., *supra* note 434, at 7.

[489] *See generally* ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984); DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW 159-87 (1994) (discussing the theory of repeated games); HOFSTADTER, *supra* note 174, at 717 (discussing the iterated Prisoner's Dilemma). *See also* Charny, *supra* note 485, at 393 ("The asset posted is the value of future dealings; if one party breaches, the other party will terminate the relationship and refuse to deal with the breacher again, destroying the asset."). For a discussion of specific variations of repeated games see, for example, Drew Fudenberg & Eric Maskin, *The Folk Theorem in Repeated Games With Discounting or With Incomplete Information*, 54 ECONOMETRICA 533 (1986); David M. Kreps et al., *Rational Cooperation in the Finitely Repeated Prisoners' Dilemma*, J. ECON. THEORY 245 (1982).

[490] *See supra* note 178.

[491] *See also* Bernstein, *supra* note 431, at 112; Greif, *supra* note 435, at 530.

[492] *See* Milgrom et al., *supra* note 434, at 1; Charny, *supra* note 485, at 393.

[493] *See* Milgrom et al., *supra* note 434, at 1. *See also* NORTH, *supra* note 143, at 55 ("Contracts will be self-enforcing when ... the benefits of living up to contracts will exceed the costs.").

[494] Charny, *supra* note 485, at 408. *See also* Klein & Leffler, *supra* note 484, at 616 ("[I]t is possible that economic agents ... may find it wealth maximizing to break such potentially long-term exchange relationships and obtain a temporary increase in profit.").

opportunistically just risks to lose the one customer it defrauded. Particularly in the context of online commerce the merchant could go on dealing with a virtually global customer base.[495]

### b) Reputation (Multilateral Reputation Mechanism)

The last point explains why *multilateral* reputation mechanisms are a much stronger tool to induce self-enforcement of contracts. When not only the defrauded individual consumer refrains from repeat transactions with a merchant, but all or at least a large group of consumers boycott that merchant, the threat of the sanction will be considerably more powerful.[496] As a consequence of such a coordinated approach, a merchant who cheats one consumer risks to deprive itself from future revenues of potential dealings with *all* consumers.[497] This mechanism is known as *collective punishment*.[498] It was, for example, successfully employed by the coalition of Maghribi traders who collectively

---

[495] *See also* Greif et al., *supra* note 436, at 751 (showing in another context that "the value of the stream of future rents collected by the ruler [herein: merchant] from an individual marginal merchant [herein: consumer] is almost zero").

[496] *Cf. id.* ("A possible means to increase the punishment is a multilateral response by all the merchants [herein: consumers] to transgressions against any subgroup of [them]"). *See also* ANNETTE BAIER, POSTURES OF THE MIND 188 (1995) ("That I won't trust you again if you break your promise to me ... is not great threat to you, if you do not need me to trust you again. But if I can have you as it were stigmatized, so that others recognize you as someone not to be trusted, then you have a fairly strong self-interested reason not to break your promise to me. ... I can harm your reputation, I can spread the word that you are not to be trusted.").

[497] *See also* Bernstein, *supra* note 432, at 112 ("when past transactional behavior is observable by a significant number of participants, breach of contract as to one transactor is transformed into breach of contract as to numerous market transactors for the purposes of a transactor's commercial reputation").

[498] *See, e.g.*, Greif, *Informal Contract Enforcement, supra* note 432, at 289.

retaliated against an agent who had cheated *one* of their members,[499] or the merchant guilds in the event of transgressions against a single member.[500]

Inducing self-enforcement of contracts by collective punishment if a merchant defects, however, is subject to specific conditions. Although examples of successful multilateral reputation mechanisms so far can mostly be found in homogenous and relatively small groups,[501] this is not a necessary precondition.[502] The factor that has limited the mechanism to small groups *as a matter of fact* was information.[503] As Greif pointed out, multilateral reputation mechanisms are doomed to fail "[i]n a world characterized by information asymmetries, slow communication, and different plausible interpretation of facts."[504] Small homogenous groups, like the coalition of Maghribi traders, are much more likely to have the social and commercial network needed to provide

---

[499] *See* Greif, *supra* note 435, at 526, 530.

[500] *See* Greif et al., *supra* note 436, at 752 (collective punishment by merchants on a city that included participation by merchants who had not been directly injured).

[501] *See* Bernstein, *supra* note 433, at 140 ("Reputation bonds are generally assumed to be effective only within geographically concentrated, homogenous groups who deal with each other in repeated transactions over the long run."); Charny, *supra* note 485, at 418 ("Collective reputational enforcement should work well in markets in which single, third-party decisionmakers wield nonlegal sanctions—that is, in markets limited to a small, homogenous group of individuals who are in frequent contact and thus can share relevant information."). Charny, *id.* at 419, also points out, however, that "[t]hese markets are, of course, relatively rare."

[502] *But see* BAIER, *supra* note 496, at 189 ("The informal enforcement of promises by withdrawal of community trust from the word of a known promise-breaker works only as long as the community is small enough for word to get around when anyone proves not to be a reliable person, not a 'man of his word.'").

[503] *See also* Milgrom et al., *supra* note 434, at 3 (pointing out that "reputations for honesty can serve as an adequate bond for honest behavior *if members of the trading community can be kept informed about each other's past behavior*") (emphasis in original).

[504] Greif, *Commercial Revolution, supra* note 432, at 129.

the information required to detect and announce cheating.[505] But it is asserted that theoretically[506] a multilateral reputation mechanism could also function in large-scale consumer markets. However, "mass markets based on reputational bonds are feasible only with technology that conveys information cheaply to a large group of transactors, such as computers used to monitor creditworthiness or mass media used in advertising."[507] Moreover, just conveying information *cheaply* is not enough. The information has to be conveyed *accurately* and must enable "other market participants [to] *discover* and *correctly analyze* the breach."[508] And while it is true that just conveying information is easier and cheaper than ever in the era of the Internet, this does not necessarily lead to "*better* and *more complete* information"[509] of consumers. With the amount of information available on the Net it has become considerably more difficult to assess its truth and to correctly analyze or simply process it.[510] People who ever typed in a keyword in one of the major search engines and then tried to figure out which of the thousands of results would be the most helpful will know that effect.

---

[505] *See id.* at 130.

[506] A study of multilateral reputation mechanisms in mass markets overcame the major problem only by *assuming* that "consumers costlessly communicate among one another" from which followed that "if a firm cheats and supplies to any individual a quality of product less than contracted for, all consumers in the market learn this and all future sales are lost." *See* Klein & Leffler, *supra* note 484, at 617. Note that the study, *id.*, found that "even such perfect interconsumer communication conditions are not sufficient to assure high quality supply"! Milgrom et al., *supra* note 434, at 3 argue that in a large community it would be too costly to keep everyone informed about what transpires in all trading relationships.

[507] Charny, *supra* note 485, at 419.

[508] *See id.* at 420.

[509] This is suggested by DIGITAL ECONOMY I, *supra* note 4, at 42.

[510] *See also* NORTH, *supra* note 143, at 23 (arguing that "the subjective and incomplete processing of information plays a critical role in decision making").

Particularly in regard to information about merchants and their past behavior it is possible that consumers will get confused by contradicting information from different sources.[511] Consider also how easy it is to spread false information for both merchants and consumers. Then, coming back to the obstacles for multilateral reputation mechanisms identified by Greif,[512] we find that slow communication is not a problem any more, but different plausible interpretations of facts—and very likely even different facts—will be a remaining problem.

In sum, while mere information *retrieval* and sharing has in fact become cheaper and easier in the Internet environment, dealing with the new flood of information, processing, organizing, assessing, analyzing, and verifying it, and picking out the useful pieces from the mass has become much more difficult and time consuming. All this suggests that a multilateral reputation mechanism in business-to-consumer electronic commerce entails enormous transaction costs. These costs are likely to render non-legal sanctions and the self-enforcement of contracts impractical unless new institutions, namely information intermediaries,[513] are able to significantly lower these transaction costs. Whether this is the case shall be discussed later.[514] For now, however, it shall

---

[511] *See also* Rothchild, *supra* note 31, at 964 ("By conveying misinformation to consumers, swindlers intend to interfere with the workings of consumer sovereignty, and they often succeed.").

[512] *See supra* note 504.

[513] *Cf.* Bernstein, *supra* note 432, at 110 (referring to trade associations as information intermediaries in some commercial relationships); Greif, *Commercial Revolution, supra* note 432, at 130 and Greif, *supra* note 435, at 526 (pointing out that the Maghribi's reputation mechanism worked only because it was coupled with a network for information transmission).

[514] *See infra* III.A.

nevertheless be assumed that some merchants will, out of reputational considerations, actually feel compelled to comply with their obligations despite the problems that multilateral reputation mechanisms face.

### c) ... And Those Who Don't Care

But there will also be a certain number of merchants who do not care about their reputation because they do not intend to build repeat-dealing relationships with customers.[515] It has been noted above that, as a matter of fact, a significant amount of merchant fraud is taking place on the Internet.[516] Online scam schemes are set up until the word spreads among consumers, then they disappear and pop up again under a different name and design.[517] This is lucrative for scam artists because the set up costs are next to zero while at the same time the Internet allows access to a global market of potential victims. Fraudulent merchants typically don't care about (and don't expect) repeated dealings with a customer,[518] they rather concentrate on tricking as many one time only consumers as possible. The main reason why such a scheme can be profitable even when its operating period is very short lies in the negligible

---

[515] *See also* Rothchild, *supra* note 31, at 964 ("Legitimate marketers recognize that a reputation for honesty is a prerequisite to long-term business success. The market provides them with a strong incentive to keep their customers happy. But perpetrators of fraud have no such interest. They do not need or expect to profit from repeat business or referrals from satisfied customers, and do not expect to remain long in the market.").

[516] *See supra* II.A.2).

[517] *See also* BAIER, *supra* note 496, at 188 (pointing out that it is fairly easy for me to assure you not to trust you again if you break your promise to me, "*unless you disguise yourself when you return with tempting offers*") (emphasis added).

[518] And even apart from fraudulent exchanges it is true that "[m]any times the exchange is a once and for all exchange and not repeated at all." *See* NORTH, *supra* note 143, at 57.

investment necessary to enter (and re-enter) the online market. It has been recognized elsewhere that "expulsion may not deter the manufacturer from breaching when the manufacturer earns a net profit from sales before reputation is devalued."[519] Multilateral reputation mechanisms do only deter a merchant from breaching when "the specific investment required of the firm to enter the market—its dedication of assets whose value would be sacrificed if the firm were later excluded from the market—[is] so great that the firm suffers a net loss when expelled from the market, even though the firm sells some defective [or nonexistent] products before the market discovers the defect."[520] And although the Internet might allow to disseminate information about past merchant behavior more quickly than ever before,[521] it lies in the nature of online transactions that there often is simply no way that information will spread quickly enough to fully avoid that online scams operate long enough to be profitable. That is, because in most cases the defrauded consumer herself will not know that she has been defrauded until a considerable amount of time has elapsed. A consumer, for example, won't realize that the goods she ordered will not arrive until a reasonable time for shipping has passed. She won't realize that her credit card account has been unduly charged until she checks her monthly statement. So even when one assumes (which is unrealistic) perfect and immediate information of all other consumers by the first victim, the fraudster will profit from other

---

[519] *See* Charny, *supra* note 485, at 413.

[520] *See id.*

[521] Subject, of course, to the limitations indicated above. *See supra* II.C.2)b).

victims during the time period until the first victim *realizes* that she has been defrauded.

## D. From Compliance to Trust?

As has been shown above, reputation mechanisms can lead to a certain degree of compliance, even to a relatively high degree of compliance—but not to a perfect one. Unfortunately, however, a high degree of compliance will not lead to a high degree of consumer trust, because whether a merchant will *actually comply* and whether a consumer can reasonably *expect* a merchant to comply are two different questions. When ninety-nine out of hundred merchants are honest and only one is a fraudster, the consumer nevertheless will mistrust all of them—unless she is able to tell *who is who* before taking the risk of entering into a transaction. Thus, a small number of dishonest merchants can disrupt consumer trust in the marketplace as a whole[522] when consumers can't distinguish the (many) good guys from the (few) bad guys. Reputation mechanisms therefore may lead to a high degree of compliance, but they are not sufficient to produce consumer trust. Trust requires more than compliance by merchants, it requires a link allowing consumers to *expect* compliance,[523] and

---

[522] In similar contexts this is referred to as a *nonidentification* problem. *See, e.g.*, Klein & Leffler, *supra* note 484, at 617 n.3 (explaining that, when a particular but unidentified firm's supply is lower than the anticipated quality, future sales will be lost not only of that firm but of all firms in the industry). *See also* Charny, *supra* note 485, at 442 (arguing that breach in one transaction may make other transactors more uncertain about whether they can trust each other).

[523] *Expectations* about another's uncertain future behavior have been identified above as being essential to trust. *See supra* text following note 175.

this link can depend on a number of different factors. The most important of these factors are information, time, and investment.

### *1) Information*

Trust, exposition to a risk because of one's positive expectations about another's uncertain future behavior,[524] is typically based on *information* about the other's *past* behavior.[525] Has this merchant complied in the past, were its customers happy? From this information potential transactors will draw inferences and build expectations as to future behavior.[526] This is problematic in several regards.

Building trust based on past behavior is the flip side of the problem whether a multilateral reputation mechanisms will induce merchants to self-enforce their obligations. Both sides are subject to the same constraints: Consumers won't trust and merchants won't comply unless the relevant information can be disseminated *and analyzed* quickly, widely, cheaply, and accurately.[527] Just the amount of information available on the Internet is likely to lead to what has been identified by Kenneth Arrow as an "efficiency loss due to informational

---

[524] For this definition of trust *see supra* text preceding note 167.

[525] *See, e.g.*, LUHMANN, *supra* note 168, at 20, 33 ("[trust] needs history as a reliable background"; "it rests on the truster ... being already informed, even if incompletely and unreliably"); GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 122-38 (discussing reasons for trust and distrust, the most important of which being information, among other things, about past actions of a person); GOVIER, SOCIAL TRUST, *supra* note 149, at 3 ("Trust presupposes beliefs, and often those beliefs are based on evidence. The case of trusting people 'immediately' or 'instinctively' is a special one, and even here we probably have evidence—we just do not reflect on what it is, or articulate it.")

[526] GOVIER, SOCIAL TRUST, *supra* note 149, at 3 ("If we know that someone has acted honestly on five occasions, we have a great tendency to infer that she will act honestly on a sixth; ....").

[527] *See supra* text following note 507.

overload."[528] Moreover, the consumer will not only face the problem of finding and filtering out the important information, she will also have to face the problem of verifying this information because never before has it been so easy to spread false or misleading information. Note also, that this information will, by the very nature of electronic commerce as being characterized by distance transactions,[529] typically not be based on the consumer's direct personal knowledge but on "media-based knowledge".[530] This raises a *secondary trust problem*.[531] Before a consumer can decide whether to trust a merchant, based on the information available to her on that merchant's past behavior, she will have to assess whether to trust the *source of information*. And recall that the source of information posted on the Internet is often not even identifiable. All this might entail very high, given the stakes involved in consumer transactions often prohibitive, transaction costs.[532]

---

[528] *See* ARROW, *supra* note 212, at 75. *See also* NORTH, *supra* note 143, at 25 (arguing that the "computational limitations of the individual are determined by the capacity of the mind to process, organize, and utilize information" and that from this "rules and procedures evolve to simplify the process").

[529] *See supra* II.A. *See also supra* text accompanying note 190 (pointing out that an important basis for trust—personal impression—is typically not available in the online context).

[530] *See* GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 124-25 (discussing media-based and knowledge arguing that it has a lower status than direct personal knowledge). *See also supra* note 189. For the implications this has *see infra* note 619 and accompanying text.

[531] *Cf.* GOVIER, DILEMMAS OF TRUST, *supra* note 149, at 124 ("The issue of media-based knowledge raises especially interesting questions of *secondary trust*: a judgment about the trustworthiness of someone we know through the media is predicated on a tacit judgment of the *trustworthiness of the media themselves*.") (emphases added).

[532] We will see later (*infra* III.A) whether new information intermediaries can significantly lower these costs.

Furthermore, even if it is assumed that a consumer can efficiently get accurate information on a merchant's past behavior, this alone is a relatively weak basis for trust. As has been shown above, "[t]he committing party will breach whenever the benefits of breach out-weigh the cost of sacrificing the bond."[533] Put differently, past behavior by itself does not really say a lot about future behavior. A merchant might always have complied in the past but find at one point, that now the benefits from breaching exceed the loss of future gains. This may be because the life cycle of the product or service is about to end, because business isn't going so well in general, because the merchant has just complied so far to establish a large enough customer base to get to the point where breaching becomes profitable and so forth. The problem therefore is that the consumer may well know about a merchant's past behavior (being compliant), but without additional information[534] she will not know whether it is *still* efficient for the merchant to be compliant in the future.

Finally, a consumer whose trust is disappointed will not be able to get any redress. The reputation of a merchant might, subject to efficient information dissemination, be ruined for the future preventing other consumers to engage into transactions with that merchant and incurring a loss. But that does not help the consumer who generated the information about the merchant's

---

[533] *See supra* note 494.

[534] *See infra* text accompanying note 544.

untrustworthiness in the first place.[535] This, of course, is simply the materialization of the risk inherent to trust and the key factor that distinguishes trust from reliance.[536]

### *2) Time*

Trust is subject to another constraint—time. Trust is built over time, based on a learning process requiring information about past behavior.[537] This process is, as Luhmann points out, "only complete when the person to be trusted has had opportunities to betray that trust and has not used them."[538] Therefore, building trust cannot only be hindered by problems of disseminating and assessing information on past behavior, but also by the lack of such information altogether, because *there is no past behavior*. Especially companies just entering the market will not have a prior record of successful or satisfying consumer transactions that is necessary for consumers to build trust. Market entrants, in fact, will not have a prior transaction record to point to at all. This becomes a major problem, when

---

[535] *See also* Charny, *supra* note 485, at 401 ("[N]onlegal sanctions may not provide ex post compensation to the victim of the breach. For example, the manufacturer's loss of reputation will not benefit the purchaser of a defective product.").

[536] LUHMANN, *supra* note 168, at 43 therefore emphasizes the need for an *investment* to start off a trust relationship.

[537] *See* The Cheskin Research & Studio Archetype/Sapient, *eCommerce Trust Study* 3 (Jan. 1999), available at <http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf> [hereinafter Cheskin Research, *Trust Study*] (characterizing trustworthiness as "a function of time and specific formal characteristics of sites" and finding that "experience is a necessity for true trust to develop"). *See also* Maryann Jones Thompson, *E-commerce Spotlight: Building Trust Online*, THE STANDARD (Jan. 25, 1999) <http://www.thestandard.com/research/metrics/display/0,2799,9928,00.html> (referring to the aforementioned study).

[538] *See id.* at 45.

*reliance* mechanisms fail as well,[539] because these could enable exchange in the absence of trust. Absent effective reliance mechanisms this *problem of initial trust* becomes fully apparent. It creates a viscous circle for new merchants: Without (initial) trust, merchants cannot build a good transaction history—and without a good transaction history, consumers won't build trust in these merchants. Without a sufficient basis for trust it is not likely that any consumer—by what would then be trusting blindly[540]—wants to be the first to put her investment at risk (with no compensation in sight if the trust is breached).[541] Thus, given the failure of traditional reliance mechanisms, overcoming the problem of initial trust is one of the greatest barriers for merchants to successfully *enter* the online marketplace. Or, as has been said elsewhere, "[e]-business is moving at the speed of light, but it is outpacing human time ... the time needed to build trust."[542]

### *3) Investment and Branding*

Given the problems of information and initial trust discussed above, two factors become extremely important in gaining consumer trust: investment and branding.

---

[539] Which, as has been shown above, they do to a large extent in the online environment.

[540] *See also* GOVIER, SOCIAL TRUST, *supra* note 149, at 3 (referring to people whose trust is not based on evidence as too trusting or gullible).

[541] *See supra* text accompanying note 535.

[542] PWC, *E-Business, supra* note 149, at 7.

As indicated above,[543] setting up shop online typically requires a significantly smaller up-front investment than doing the same thing offline. This is one reason why the online marketplace is such an attractive place for scam artists. The expenditures for honest merchants might be higher than for fraudsters—depending on the goods or services offered—since they eventually need to get and store supplies, rent storage facilities etc. However, even where online merchants incur these costs, it is typically not visible to customers. This accounts for one important difference between online and offline shops. Offline the customer can get a personal impression of the physical location which had to be rented, the goods that are displayed etc.[544] All this conveys additional information to the consumer, namely information about a merchants *initial investment* or its *sunk costs*. This information is important in regard to the above finding that self-enforcement of contracts will fail, when the benefits of breaching and reaping a short-run profit outweigh the costs of sacrificing potential future profits from repeated transactions.[545] A firm's initial investment plays an important role in this equation. The higher the sunk costs at the beginning, the more the merchant becomes dependant on an anticipated future revenue stream from repeated dealings because breaching and pulling out of the market will overall not be profitable unless the sunk costs of setting up the venture have been recovered. Thus, a consumer's knowledge about a merchant's sunk costs will strengthen her

---

[543] *See supra* note 114 and accompanying text.

[544] *See also supra* note 29 and accompanying text.

[545] *See supra* note 494.

trust in that merchant's compliance.[546] Online, however, there will either be next to no investment in physical assets at all or information about such an investment will not be visible for consumers.[547] Nevertheless, there are other ways of "buying" trust that also work in the online world, namely *expenditures on advertising* and establishing a well known brand name.

Klein and Leffler have shown that "brand-name capital" investments (for example sunk investments in the design of a firm logo or an expensive sign promoting the firm's name) can serve as a hostage to prevent a merchant from cheating.[548] They argue that advertising supplies valuable information to consumers, most importantly the information "*that the firm is advertising*".[549] Advertising, information about past advertising, or the publication of large fees paid to celebrities for commercials,[550] inform consumers[551] about the magnitude of sunk capital costs. If the investment is sufficient, it "implies that a firm will not engage

---

[546] This is the additional information referred to *supra* text accompanying note 534.

[547] Some investments in the "shop", however, may also be visible online. This includes expenditures on a sophisticated design of the site, expenditures on cutting edge technology leading to fast and reliable accessibility etc. This explains why easy navigation, professional presentation, and state of the art technology have been found to be among six primary components communicating trust online. *See* Cheskin Research, *Trust Study, supra* note 537, at 9.

[548] *See* Klein & Leffler, *supra* note 484, at 626.

[549] *See id.* at 630.

[550] Note that a number of online companies meanwhile use celebrity endorsed commercials, for example: William Shatner (Priceline.com), Cindy Crawford (babystyle.com), Whoopi Goldberg (Flooz.com), Anna Nicole Smith (E*Trade), Picabo Street, Anna Kournikowa (Charles Schwab), Geena Davis, Jackie Chan, Phil Jackson (TD Waterhouse), Shaquille O'Neal, Tiger Woods, Michael Jordan (SportsLine), Sammy Sosa (OneNetNow.com). *See* Toni Logan, *Lights! Camera! Stock Options! Celebrities help ebusinesses build brand, but can star power substitute for an integrated marketing strategy?*, BUSINESS 2.0, April 2000, at 165.

in short-run quality deception since the advertising indicates a nonsalvageable cost gap between price and production costs".[552] In other words "consumers know that such sunk costs can be profitable only if the future quasi rents are large."[553] And if consumers estimate that the initial sunk expenditure is greater than the short-run cheating gain, "then a price premium on future sales sufficient to prevent cheating is estimated to exist."[554] In short, if a company spends enough on advertising and building a brand, consumers can be confident that this company will not be going for the short-run profit by cheating—simply because it doesn't pay.

Thus, by making a large enough investment (i.e. by "sinking" enough costs) up-front, companies can "buy" consumer trust. More importantly, the company can buy *initial* trust. It doesn't need a good record of prior transactions for this formula to function. The "classic" example of an online merchant that took this route is Amazon.com.[555] Revenues grew from $15.7 million in 1996 to $1.6 billion in 1999. The fact that Amazon.com still reported a net loss that went up from $5.8 million in 1996 to $719 million in 1999 is partly due to extensive expenditures on branding and advertising[556] to build a loyal customer base.[557] These efforts have

---

[551] Klein & Leffler explicitly state that they "do not want to claim that consumers 'know' this theory in the sense that they can verbalize it but only that they behave in such a way as if they recognize the forces at work." *See id.* at 634.

[552] *See id.* at 630.

[553] *See id.* at 631.

[554] *See id.*

[555] *See* http://www.amazon.com.

[556] *See* Robert Spector, *Going for Broke*, BUSINESS 2.0, April 2000, at 256, 262.

obviously been successful since Amazon is found to be one of the best known and, more importantly, one of the most trusted web brands.[558] The customer base grew from 180,000 in 1996 to 17 million in 1999.[559] Amazon's core segments—music, DVD/video, and books—have meanwhile achieved profitability, and the company as a whole is expected to be profitable by 2002.[560]

It is therefore not surprising that several studies on online commerce mention a company's *brand* as one of the most important factors in the process of building trust.[561] The most trusted brands have been found to all be well-known brands,[562] implying considerable capital investment in building the brand and *making* it well known.

Given the importance of a well-known brand it is also clear that existing bricks and mortar stores that already have established a brand and a reputation can have an important advantage as they go online and evolve to *clicks and mortar* stores. The finding that "brand matters more than medium" which is underlying the argument that well known e-brands could now also successfully operate in

---

[557] Richard Richtmyer, *Amazon beats the Street: Online retailer sneaks past estimates; sees narrower operating losses*, CNNfn (April 26, 2000) <http://cnnfn.com/2000/04/26/technology/amazon>.

[558] *See* Cheskin Research, *Trust Study, supra* note 537, at 20.

[559] It is reported to have reached 20 million as of March 31, 2000. *See* Richtmyer, *supra* note 557.

[560] *See id*.

[561] *See* PWC, *E-Business, supra* note 149, at 10; Cheskin Research, *Trust Study, supra* note 537, at 9. *See also* DIGITAL ECONOMY I, *supra* note 4, at 25 ("Building brand awareness through advertising and marketing is critical to success in a new and rapidly evolving market, ....").

[562] *See* Cheskin Research, *Trust Study, supra* note 537, at 20 (listing the 12 most trusted brands, starting with Yahoo!, Wal-Mart, and Netscape).

the physical world,[563] is also true in the opposite sense. Offline stores can leverage their existing reputation online.[564] An offline presence further implies visible tangible assets (and investments in those) which are an additional factor in the process of building trust.[565] Consequently studies suggest that five of the twelve most trusted brand names in e-commerce originate offline (including Wal-Mart, Blockbuster Video, USA Today, and Dell), while none of the least-trusted sites does.[566]

Another survey showed that 39% of all users and 46% of new users (being online for less than a year) are generally more likely to shop from merchants they have bought from offline.[567] In other words, offline companies have already made the investment in branding and advertising that is important to overcome the problem of initial trust. Moreover, because they do have a physical and visible presence, other bases for trust and reliance become more important. These factors include the existence of and possibility to actually reach tangible assets, the possibility of getting a personal impression, or the greater difficulty of escaping law enforcement. Thus, the absence of anonymity, mobility, and globality—characteristics of the online world—in the offline world makes it generally easier

---

[563] *See id.* at 30.

[564] *See* PWC, *E-Business, supra* note 149, at 23 ("[C]ompanies that *have* made good on their promises, that *do* have strong track records on Main Street and in cyber-space, *are* the ones that can move forward into cutting-edge areas. They proceed, confident of drawing interest because they have developed a measure of trust over the years that will stand them in good stead as innovative measures are undertaken online.").

[565] *See supra* text accompanying note 547.

[566] *See* Cheskin Research, *Trust Study, supra* note 537, at 4, 20.

[567] *See* Guglielmo, *supra* note 123 (citing a survey by Jupiter Communications).

to establish consumer confidence offline. When going online, initial trust is not a problem for these companies. Pure online merchants, however, start from scratch in the new environment. They do face the problem of initial trust and can not rely on these other factors to overcome it. Expenditures on branding and advertising therefore become relatively more important to build initial trust.

Once the barrier of lacking initial trust is overcome, be it offline or by means of "sinking costs" online, the vicious circle is broken up. The company now has the chance to build a track record. Consumers will make experiences, and a history of successfully completed transactions can develop.[568]

## E. Who Gets Left Behind?

Building trust online is more difficult than offline—but it is obviously possible. Why, then, can't it all be left to the market—apart from the fact that almost everybody, including the market participants, agrees[569] that the lack of consumer confidence is one of the greatest barriers for electronic commerce to reach its full potential?

Given the above findings it is apparent that traditional reliance mechanisms—to the largest extent—do not work online. Regarding trust, the biggest problem is an inherent lack of initial trust. Adding these two findings together implies that, in the extreme, consumers avoid transactions with new and unknown online merchants

---

[568] *See* PWC, *E-Business, supra* note 149, at 10.

[569] *See supra* notes 13-21 and accompanying text.

altogether. The problem of initial trust can be overcome if a bricks and mortar company can leverage its offline brand to the online environment, or if an online company can afford high expenditures on advertising and branding to inform consumers of a significant amount of sunk costs and thus give them a reasonable basis to trust in subsequent compliance by that company, because it needs to recover these losses by establishing repeat-dealing relationships with customers.

So who gets left behind under these conditions? For once, those merchants get left behind that do not have a well known offline brand, that do not have the financial means to make enormous up-front investments in branding and advertising, and that cannot afford to lose money for 6 to 7 years before eventually becoming profitable. Recent developments show, that an increasing number of companies do not have the long (financial) breath required to take the route of "buying trust" over an "amazonian" period of about 7 years before producing black numbers on their balance sheet. As more and more online retailers or e-tailers run short on cash because sales are lower than expected while "[a]t the same time, they've poured millions of dollars into expensive advertising campaigns in a desperate attempt to establish brand names",[570] public investors as well as venture capitalists are getting more skeptical.[571]

---

[570] *See also* Joelle Tessler & Matt Marshall, *Online firms short on cash*, SAN JOSE MERCURY NEWS, April 1, 2000, A1.

[571] *See id.* (citing Lior E. Yahalomi of CMGI@Ventures.com, a venture capitalist specializing in Internet companies, as saying that fewer business-to-consumer Internet companies are meeting the more stringent investment criteria that his firm is now using).

New market entrants that cannot leverage an offline reputation or "buy" online trust, however, are trapped in the vicious circle described above: Absent effective reliance mechanisms they absolutely depend on a record of prior transactions as a basis for consumer trust—without already having established trust, however, consumers will not engage in transactions with the merchant in the first place. The lack of (initial) consumer confidence thus creates a high entry barrier for new merchants, particularly for small and medium sized enterprises (SMEs).[572] Less than one third of SMEs with a web presence[573] are using their sites to sell products, provide customer support, or reduce operating costs.[574] Exactly these enterprises, however, are frequently believed to play a crucial role in the further development of electronic commerce.[575] Vice president Al Gore even asserts "that small and medium-sized enterprises, and their rapid adoption of e-commerce, are crucial to our continued economic success."[576] Facilitating small business participation in electronic commerce therefore has been an explicitly

---

[572] This fact is overlooked by OECD, *supra* note 464, at 39 (asserting that "[t]he Internet has made it easier for both SMEs and individuals to enter the marketplace, as they need neither physical shops nor sales offices").

[573] A survey by The Yankee Group finds that 28% of companies with less than 20 employees, 54% of companies with between 20 and 99 employees, and 62% of companies with between 199 and 499 employees maintain a web presence, *see* WORKING GROUP II, *supra* note 4, at 25 n.29.

[574] *See id.*

[575] *See generally* OECD, Directorate for Science, Technology and Industry, Industry Committee, Working Party on Small and Medium-Sized Enterprises, *SMEs and Electronic Commerce*, DSTI/IND/PME(98)18/REV1 (Sept. 18, 1998) <http://www.oecd.org/dsti/sti/it/ec/prod/sme18e.pdf>.

[576] *See* WORKING GROUP II, *supra* note 4, at ii.

stated policy goal in the U.S. as well as in Europe.[577] Without establishing *initial* consumer confidence, however, the achievement of this goal seems endangered.

In addition to the entry barriers for SMEs, the few (larger) companies that could leverage their offline brand or successfully made high investments in establishing their online brand get a double advantage. They can overcome the lack of initial trust and, now getting the chance to engage in repeated transactions, they can build a positive track record and ultimately a good reputation. Once having made a good experience with an online merchant, customers are likely to come back to that merchant instead of taking the risk of trying out a new merchant. According to a survey 37% of customers will favor merchants they have bought from before.[578] Other findings suggest an even higher percentage of returning customers. Repeat-customer orders, for example, represented 76% of Amazon's total orders in the first quarter of 2000.[579] This suggests that the first-mover advantage of those overcoming the initial trust problem is becoming more important than ever.

---

[577] *See id.* at iv, 26-28 (describing various initiatives of the U.S. Department of Commerce and other agencies to assist small companies in the use of electronic commerce); *A European Initiative in Electronic Commerce, supra* note 16, at 4 ("Electronic commerce presents enormous potential opportunities for consumers and for businesses in Europe, *particularly for SMEs*.") (emphasis added) (continuing to describe the particular importance of SMEs and special programs to support SMEs involvement in e-commerce throughout the document).

[578] *See* Guglielmo, *supra* note 123 (citing a Jupiter Communications research).

[579] *See* Richtmyer, *supra* note 557 (this number is up from 66% during the same period in 1999).

The big get bigger and the small will have an increasingly harder time to enter the market and compete. This does not only effect pure online companies,[580] but also small offline merchants. The latter are in a dilemma. For the reasons described above they will have a hard time entering the electronic marketplace, and—imagine a small book shop—they increasingly run the risk to lose market share against online retailers like Amazon, because people find it more convenient to shop online. It has been noted before, that the brand now often matters more than the medium,[581] meaning online companies are also competing with their offline counterparts. Therefore, "[b]y not making the transition to this new way of doing business, small firms run a serious risk of becoming less competitive, affecting both their present market positions and long-term viability."[582] Given a lack of initial consumer confidence, however, making that transition is not all that easy.

Besides SMEs and market entrants with modest financial means, consumers may get left behind to some extent as well. In the situation just described, the diversity of the market may suffer, ultimately limiting the consumer's choice. If you, for some reason, do not want to buy your books at Amazon but the bookstore at the corner, you might find that the store did not make it, neither online nor offline. The whole idea of the Internet making possible a highly diverse

---

[580] For an example see Tessler & Marshall, *supra* note 570 ("The company [CDNow] has been struggling ever since Amazon.com began selling music online in the summer of 1998 and quickly became the largest music retailer on the Web.").

[581] *See supra* note 563.

[582] WORKING GROUP II, *supra* note 4, at 25.

market where everybody—large companies, SMEs, or individuals—can be a buyer and a seller and transactors find the best match each time, stands and falls with the existence of initial confidence. Without it, consumers will have no choice but to become repeat customers, always coming back to the few companies that could overcome the initial trust barrier. Trying other (new or small) companies and their products and services will remain a risky business, meaning that a number of consumers will refrain from doing it although they might get a better deal if the transaction was successful.

Finally, even where companies can overcome the problem of a lack of initial trust, for example by making high up-front expenditures on branding and advertising, the consumer's position remains rather weak. Trust relationships, no matter on which bases the trust is grounded, always remain risky. This aspect distinguishes trust from reliance.[583] If the consumer's trust is breached, the merchant might face a loss of reputation, but the individual consumer won't be able to get redress.[584] To some extent, therefore, the trusting consumer is always at the merchant's mercy. Ultimately it is the merchant who decides when breaching the consumer's trust is efficient. Even with a stronger basis for trust, like high initial sunk costs, the consumer depends on the merchant getting his economics right. When it is clear that the business, despite—or because—the high initial investment will never be profitable, the merchant can play an end game and try to at least reap all the short-run profits it can by cheating.

## F. Summary—The Need for New Institutions

To serve as a basis for consumer reliance, enforcement mechanisms must be actually *effective*, *cheap*, and *quick*. Moreover, they must be able to guarantee a consumer individual *redress* if things go wrong and they must be available *upon the consumer's own initiative*. The above analysis has shown that traditional enforcement mechanisms as currently employed generally don't meet these requirements. Litigation is too expensive. State enforcement will be ineffective to a certain extent because of problems in detecting fraudulent behavior, tracking the person behind it, and reaching this person or assets within the jurisdictional boundaries of the enforcement agency. Moreover, criminal sanctions—as organization enforcement—will not lead to redress of an individual defrauded consumer. Further, all third party enforcement mechanisms (criminal sanctions, FTC actions, and organization enforcement) are *not* initiated by the consumer. The consumer depends on the third party to make the decision to bring an enforcement action. This decision depends on a variety of factors beyond the consumer's control (costs, feasibility, prospective of success, magnitude of damage, etc.). Thus, even where consumer redress is theoretically possible (as in FTC actions), these mechanisms remain a very weak basis for an individual consumer's confidence that things can be fixed *for her* if they go wrong.

---

[583] *See supra* notes 175, 198 and accompanying text.

[584] *See supra* note 536 and accompanying text.

The second basis of consumer confidence—trust—faces its limits as well. It is subject to significant constraints regarding availability, verification, and assessment of information. To some extent these information deficiencies can be overcome by high investments of merchants, but this option clearly is not available to everyone. Trust also has other limits of a more general nature. Most importantly, the consumer is always left at the merchant's "mercy" to the extent that the merchant is likely to breach the consumer's trust the moment it becomes more efficient than living up to it. The information asymmetries in regard to the factors determining that decision are typically even larger.

This situation suggests a need for new institutions[585] that enable and facilitate building consumer confidence by overcoming the problems identified above. The types of new institutions that emerge or could emerge and the ways in which

---

[585] *See also* NORTH, *supra* note 143; at 33 ("[W]ithout institutional constraints, self-interested behavior will foreclose complex exchange, because of the uncertainty that the other party will find it in his or her interest to live up to the agreement."), 34 (stressing the need for reliable institutions that allow individuals to engage in complex contracting); BAIER, *supra* note 496, at 189 (Discussing and restating Hume's argument for the need of institutions: "Only when magistrates are invented to receive complaints and to keep official track of a person's record can persons in a large society count on a promise-breaker being generally know as such, and/or effectively punished."). *See generally* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM 163-205 (1985) (discussing institutions and "credible commitments").

these institutions try to enhance consumer confidence will be discussed in the following section.

## III. ENHANCING CONSUMER CONFIDENCE: THE RISE OF NEW EXTERNAL INSTITUTIONS

In the literature the role of institutions has been emphasized both for overcoming information problems[586] and providing third-party enforcement.[587] Simple reputation mechanisms, for example, require keeping every transactor completely informed about everybody else's past behavior.[588] While this was possible within small, homogenous groups engaging in local trade,[589] it quickly becomes too costly in regard to large-scale impersonal exchange.[590] It becomes too costly *unless* institutions, namely information intermediaries, can significantly mitigate the information costs.[591]

Others assert that in complex societies engaging in large-scale impersonal exchange, neither self-enforcement nor trust can be completely successful and a coercive third party that enforces agreements is essential.[592]

---

[586] *See, e.g.*, Milgrom et al., *supra* note 434, at 2 ("[W]hat role do formal institutions play when simple reputational mechanisms fail?").

[587] *See, e.g.*, NORTH, *supra* note 143, at 58 ("[V]iable impersonal exchange that would realize the gains from trade inherent in the technologies of modern interdependent economies requires institutions that can enforce agreements by the threat of coercion.").

[588] *See* Milgrom et al., *supra* note 434, at 3. *See also supra* note 503.

[589] *See, e.g.*, NORTH, *supra* note 143, at 34 ("personalized exchange involving small-scale production and local trade"). *See also supra* note 501.

[590] *See* Milgrom et al., *supra* note 434, at 3 ("In a large community ... it would be too costly to keep everyone informed about what transpires in all trading relationships, ....").

[591] *See supra* note 513 and accompanying text. *See also* Milgrom et al., *supra* note 434, at 7.

[592] *See* NORTH, *supra* note 143, at 35.

Both approaches, self-enforcement as a basis for trust and third-party enforcement as a basis for reliance, in their traditional forms have been shown to not meet the needs of the online marketplace—the classic example for large-scale impersonal exchange. Both approaches, however, using new mechanisms, attempt to overcome the problems and adapt to the online environment. Thus, one can observe the emergence of new institutions that ultimately aim at fostering trust, namely information intermediaries, and new institutions trying to provide effective third-party enforcement and foster reliance.[593] Recalling the economics of trust and reliance discussed above,[594] the central question becomes which of these approaches can enhance consumer confidence—if at all—more efficiently.

## A. New Institutions to Foster Trust—Information Intermediaries

The institutions that try to make bi- and multilateral reputation mechanisms work in the online environment[595] are information intermediaries. A multitude of different approaches can currently be observed in the market. The intermediaries typically convey information about merchants that is supposed to serve as a

---

[593] *See also* Heckman, *supra* note 113, at 2.8 (emphasizing that "[i]ntermediaries may also emerge as the answer for enabling consumers to recover damages").

[594] *See supra* II.B.1)c).

[595] *See supra* notes 514, 532 and accompanying text.

basis for consumers to establish trust.[596] Most of these approaches, however, face similar limits.

### *1) The Approaches*

Information intermediaries that provide information on online merchants and their business practices to assess their trustworthiness are numerous. Listings of "*selected*" reliability programs, issuers of seals of approval, or rating services include more than 75 such services,[597] and new ones seem to appear daily.[598] The following will provide an overview on some of the better known services.

#### a) BBBOnline Reliability Program

The Better Business Bureau offers an online reliability seal program "to help web users find reliable, trustworthy businesses online, and to help reliable businesses identify themselves as such."[599] Merchants who want to use the BBBOnline reliability seal must meet certain standards.[600] They will have to become a member of the Better Business Bureau, provide the BBB with information regarding company ownership and management and its physical address (which

---

[596] *See supra* II.D.1) for the role of information in the process of building trust.

[597] *See* Alliance for Global Business, *supra* note 17, at 42-84 (listing and comparing selected initiatives). *See also* Cheskin Research, *Trust Study, supra* note 537, at 16 (listing the 27 security brands "that matter most"). *See also* WORKING GROUP II, *supra* note 4, at 12 (describing seal programs such as BBBOnline and CPA WebTrust).

[598] A more recent occurrence, for example, is PriceWaterhouseCoopers' BetterWeb Seal that costs a merchant $15,000 per website per year. *See* PriceWaterhouseCoopers, *The BetterWeb Program* (visited Aug. 17, 00) <http://pwcbetterweb.com>.

[599] *See* BBBOnline, *Reliability Program* (visited Aug. 17, 00) <http://www.bbbonline.com/businesses/reliability/index.html>.

[600] *See* BBBOnline, *Standards for BBBOnline Reliability Program Participation* (visited Aug. 17, 00) <http://www.bbbonline.com/businesses/reliability/standards.html>.

will be verified by the BBB), they must be in business for a minimum of one year, they must have a satisfactory complaint handling record with the BBB, they must agree to participate in the BBB's advertising self-regulation, and they must agree to dispute resolution at the consumer's request. The BBB, however, explicitly notes that it does not guarantee that customers will be satisfied with the merchant's product or service, or that the merchant never experienced complaints or will so in the future. The BBB does not pre-clear or pre-approve any advertising of the participants, nor does it engage in active monitoring or bring enforcement actions if a merchant violates the BBB standards. Annual fees for participating merchants range from $100 to $3000 depending on the size of the company.

**b) CPA WebTrust**

The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants issue the CPA WebTrust seal[601] because "it's difficult to judge a company's honesty and integrity simply by looking at a website."[602] To get the seal, the company's website is examined by a specially licensed certified public accountant (CPA) who will, among other things, evaluate its business practices, including order processing, and handling of returns, warranties, and other problems. The business practices must meet the standards set forth in the CPA WebTrust Principles and Criteria for Business-to-Consumer Electronic

---

[601] *See CPA WebTrust* (visited Aug. 17, 00) <http://www.cpawebtrust.com>.

[602] CPA WebTrust, *It's a Matter of Trust* (visited Aug. 17, 00) <http://www.cpawebtrust.com/consumer/index.html>.

Commerce.[603] These principles require, among other things, that the company's management maintains effective controls to provide that customers' orders placed were completed and billed as agreed.[604] To keep the seal the site must be re-audited by a CPA every ninety days and show that it is in conformity with the WebTrust standards.

PriceWaterhouseCoopers' BetterWeb Program operates in a quite similar manner.[605] The fee for the BetterWeb seal is $15,000 annually.

### c) Bizrate, eComplaints, and e-Rating

Bizrate.com,[606] eComplaints.com,[607] and Consumer Reports Online's e-Ratings[608] take a slightly different approach from the seal programs discussed above.

Bizrate is ranking online merchants according to their performance ratings by actual customers. The information includes the buying process itself and whether the delivery arrived on time and met the customer's expectations. Customers,

---

[603] *See* American Institute of Certified Public Accountants, Inc. & Canadian Institute of Chartered Accountants, *Web Trust Principles and Criteria for Business-to-Consumer Electronic Commerce* (Oct. 15, 1999) <http://www.aicpa.org/webtrust/princritb.htm>.

[604] For a detailed list of the Criteria the company has to demonstrate that it is conformity with see *id.* <http://www.aicpa.org/webtrust/wtpcbprinc.htm>.

[605] *See supra* note 598.

[606] *See* <http://www.bizrate.com>.

[607] *See* <http://www.ecomplaints.com>.

[608] *See* <http://www.consumerreports.org>.

according to a list of ten criteria regarding the merchant's business practices,[609] then rate the stores. Bizrate thus is a typical information intermediary that collects and aggregates customers' information on past transactions.[610]

Ecomplaints.com collects consumer complaints about companies based on the consumers' own experiences and publishes them on the web "to provide information to potential consumers before they purchase a product or service in order to reduce their own risk".[611] Shoppers are encouraged to "stop in at eComplaints.com and read the complaints other consumers have issued" before they buy.[612]

Consumer Reports Online does not rely on customer information for its e-Ratings, but it frequently evaluates sites on its own by approaching them "as an average customer would."[613] The store is then rated according to a checklist, which includes policies, usability, and content. The ratings are only accessible for

---

[609] *See* Bizrate.com, *About BizRate.com—Store Ratings* (visited Aug. 17, 00) <http://www.bizrate.com/inside/ratings.xpml>.

[610] Ebay's Feedback Forum takes a similar approach in the consumer-to-consumer environment. *See* Ebay, *The Feedback Forum* (visited Aug. 17, 00) <http://pages.ebay.com/services/forum/feedback.html>.

The idea is also quite similar to institutions that have evolved to overcome information problems regarding medieval champagne fairs and that have been studied by Milgrom et al., *supra* note 434. In both cases "each individual possesses direct information *solely about his own past trading experiences*." (*See id.* at 9). The law merchant system that has developed in response to that (each transactor shared her information with a private judge who also serves as a repository for information, *see id.* at 10) is, in fact, an early example of a feedback forum.

[611] *See* eComplaints.com (visited Aug. 17, 00) <http://www.ecomplaints.com/About/about.php3>

[612] *See* eComplaints.com (visited Aug. 17, 00) <http://www.ecomplaints.com/index.php3>.

[613] *See* Consumer Reports Online, *e-Ratings Online Shopping Guide* (visited Aug. 17, 00) <http://www.consumerreports.org/Special/Samples/Reports/0001erat.htm>.

subscribers.[614] In principle, Consumer Reports Online's approach is not much different from Bizrate's except that the former generates its own information about a specific merchant while the latter relies on information provided by customers.

### *2) The Limits*

The most obvious limit of all of the approaches described above is that they cannot overcome the problem of lacking *initial trust*. Information intermediaries generally depend on existing information about merchants' past transactions. This is the reason why BBBOnline requires a merchant to be in business for at least a year before it can be considered for the reliability seal. CPA WebTrust requires merchants to make representations that can be verified regarding a period of 2 to 4 months preceding the application. Rating and feedback services by their very nature rely on customer information about their transaction experience with a merchant. Consumer Reports Online is an exception in this respect because it generates information on its own by engaging in test-transactions.

Another problem is that the sheer mass of seal programs and rating services[615] is likely to confuse consumers. Surveys have shown that, for example, only 18% of users are familiar with BBBOnline and that even less, 8% of users, are familiar

---

[614] The rate is $3.95 per month or $24 per year.

[615] *See supra* note 597.

with Bizrate.[616] It has been found that "security brands" are generally not well known to consumers.[617] This situation aggravates the *secondary trust problem* briefly addressed above.[618] A consumer will not trust a seal that she does not even know. So first, she would have to establish trust in the intermediary providing the seal, which entails information costs. And the more seals and ratings there are, the greater is the danger of dilution. Moreover, different programs have different standards and verification procedures. Ecomplaints or Bizrate, for example, apparently do not verify the information that users give them.[619] Thus, the whole problem of wrong or contradicting information on the net is not solved and the consumer hardly has a meaningful basis for assessing a merchant's trustworthiness. A consumer would first have to educate herself as to the different standards, controls, or enforcement mechanisms employed by a particular intermediary. She needs to ask herself whether she can trust this site *and* whether she can trust this seal. The information problem is just transferred to another level.

And even if a consumer does rely on a specific service, all of the mechanisms discussed above still entail significant transaction costs. Services like Bizrate or eComplaints rely on consumers reading through the complaints or ratings before they shop. This takes time and makes the buying process cumbersome.

---

[616] *See* Cheskin Research, *Trust Study, supra* note 537, at 16

[617] *See id.* at 15.

[618] *See supra* note 531 and accompanying text.

[619] *See also supra* notes 189, 530 (discussing media-based knowledge as opposed to direct personal knowledge).

Presumably buyers would prefer not to read through numerous complaints of other customers about a particular merchant (not even knowing whether these complaints are true or not) before making the decision to engage in a transaction with that merchant. Thus, it is likely that they stick with the merchants they know, with the well-known brands. It has been observed elsewhere that "[p]eople will make seemingly irrational choices because the costs of acquiring better information outweigh the benefits they expect from it" and that "[i]t is not rational for people to be 'rational' about every single choice they make in life; if this were true, their lives would be consumed in decisions over the smallest matters."[620] Thus, if it can be avoided, a consumer would rather shop without having to look through what others have said about the merchant she is about to shop with. The same is true in regard to acquiring information about a trust seal displayed on a merchant's site. Seal programs entail yet other transaction costs. Auditing and frequent re-auditing of websites and business practices by a certified public accountant or a consultant is expensive. An annual fee of $15,000, for example, does not seem to be a negligible expenditure for a small enterprise trying to get online.

Finally, despite all the seals and ratings the risk that the merchant will defect *in the future* remains. This risk is inherent to any transaction based on trust[621] and

---

[620] FUKUYAMA, *supra* note 145, at 20.

[621] *See supra* note 535 and accompanying text.

is to be included in the costs of trusting when they are compared to the costs of reliance on (effective) enforcement mechanisms.[622]

## B. Reliance on New Enforcement Institutions—The Crucial Role of Payment Intermediaries

The limits of using information intermediaries to foster trust and the costs this approach entails suggest looking at another alternative. If establishing trust is too expensive and the risks that remain are too great,[623] one could turn towards enhancing reliance instead. Since consumer confidence will follow from both trust or reliance, the more efficient of the two should be chosen. The structure of online transactions reveals an enforcement approach that might be *effective* and significantly *less costly* than the attempts to enhance consumer trust while, at the same time, it could guarantee *initial* consumer confidence regarding any transaction without the need for any information on that particular merchant.

This approach addresses *payment intermediaries*. Due to the nature of online transactions as distance transactions, which precludes an on-the-spot exchange of the goods or services provided by the merchant and the customer's consideration, all of these transactions involve a payment intermediary. This can be a credit card issuer, a bank that has to clear a check, or an e-cash or

---

[622] *See supra* II.B.1)c).

[623] NORTH, *supra* note 143, at 35 suggests that "neither self-enforcement by parties nor trust can be completely successful" and that, since "the returns on opportunism, cheating, and shirking rise in complex societies", a "coercive third party is essential."

cybercash provider.[624] The payment intermediary has an important middle position in the transaction. The market has recognized this key role of payment providers in the context of efforts to enhance consumer confidence and a variety of services have developed that try to leverage this position. Legislators, particularly outside the U.S., so far have recognized the strength of chargeback mechanisms only to a limited extent. If they want to foster consumer confidence in the electronic marketplace, this paper argues that they should employ chargeback obligations as a means of enforcement of consumer rights more broadly.

### *1) Market Approaches*

Several market approaches currently make use of the crucial role of payment providers described above. Their objective is to mitigate the risk of prior performance and to overcome the lack of effective enforcement of consumer rights by affording quick, cheap, and easy redress to consumers if things go wrong.

#### a) Escrows

The first group of services that specifically address the risk of prior performance normally born by the consumer, are escrow services such as escrow.com[625] or iescrow.com.[626] The goal of these services is to "reduce the risk of fraud for

---

[624] *See supra* note 95 for an overview on online payment systems.

[625] *See* <www.escrow.com>.

[626] *See* <www.iescrow.com>.

parties buying or selling merchandise from each other over the Internet" and to "ensure buyers get what they pay for."[627] Basically, a third party—the escrow service—receives the buyer's payment, verifies it, and holds it in escrow until the buyer has received and inspected the merchandise. If the buyer is satisfied, the escrow service releases the payment to the seller.[628] If the buyer is not satisfied the escrow service releases the payment back to her, once the seller has received the returned merchandise. Both parties must register with the escrow service and enter into an escrow agreement before the transaction. The escrow fee normally ranges between 1% and 4% of the value depending on its magnitude and the payment mechanism used.[629]

These services, at the cost of needing to register, making an additional agreement, and paying the escrow fees, overcome the lack of *initial confidence*. The consumer's risk is mitigated because she gets her money back (less the escrow fee, of course) if the merchandise is not delivered as agreed upon. In the words of iescrow.com the service can "allay fears of buyers wary of unknown sellers"[630] and thus overcome the problem of limited brand awareness for those

---

[627] *See id.*

[628] *See* escrow.com, *The Escrow Process* (visited Aug. 17, 00) <http://www.escrow.com/overview/index.html>. *See also* iescrow.com, *Financial Questions* (visited Aug. 17, 00) <http://www.iescrow.com/finfaq.html#cost>.

[629] *See* escrow.com, *Escrow Fee and Transaction Management Fee* (visited Aug. 17, 00) <http://www.escrow.com/help/fees.html>.

[630] *See* iescrow.com, *The Smart Way to Shop Online* (visited Aug. 17, 00) <http://www.iescrow.com/service.html>.

who do not have the funds to "buy" consumer trust with high investments in branding.[631]

### b) "Blue," Shopping Guarantees, and Insurance

Another approach is Blue from American Express.[632] Blue is a credit card with "special online features." These include an "online shopping guarantee", which means that Blue users who use the card online will not be held responsible for any unauthorized charges.[633] The return protection allows users to return any item they bought online even if the merchant won't take it back—American Express will refund the user up to $300 per item and $1000 per year. These guarantees and protections obviously aim at fostering consumer reliance in the electronic marketplace.

Online shopping insurance policies pursue the same goal. Ebay users, for example, benefit from ebay's free insurance for any item up to $200.[634] The insurance will cover losses resulting of payment for an item that is never received or that is less than what is described. The German Insurance Company Gerling[635] is offering something similar. Its e-commerce insurance covers the risk

---

[631] *See supra* II.D.3).

[632] *See* American Express, *You've Got Blue* (visited Aug. 17, 00) <http://home4.americanexpress.com/blue/card_home.asp>.

[633] It is not really clear, however, what "unauthorized" means in this context. If it covered only fraudulent third party use of the card data, this guarantee would in effect not go beyond what it required by law anyway. *See supra* note 64 and accompanying text.

[634] *See* Ebay, *Fraud Prevention & Insurance* (visited Aug. 17, 00) <http://pages.ebay.com/help/community/insurance.html>.

[635] *See* <http://www.gerling.de>.

that merchandise is never delivered or that it is defective. Participating shops, which in return get a "Trusted Shop" seal, pay the premium.[636] The consumer buying from these Trusted Shops gets a money-back guarantee from Gerling if anything goes wrong in the transaction.

### *2) A Policy Perspective—Addressing Payment Intermediaries and Introducing Chargeback Mechanisms*

It remains to be seen whether these market approaches—and others that are sure to come—will be successful. Since they represent *reliance* mechanisms they are not subject to most of the doubts expressed above in regard to information intermediaries trying to foster consumer *trust*. It is another question, whether policy makers, who want to accelerate the development of electronic commerce will or should consider similar approaches. One such example of a chargeback regime that has been introduced by the legislator actually exists: the U.S. credit card regulation.

#### a) Chargebacks in U.S. Credit Card Regulation

As indicated above, in the U.S. the use of credit cards is mainly regulated by the Truth-in-Lending Act (TILA)[637] and the Federal Reserve Board's implementing Regulation Z.[638] These regulations go beyond protecting the consumer from

---

[636] *See* Trusted Shops <http://www.trustedshops.de>.

[637] *See supra* note 59.

[638] 12 C.F.R part 226 (1999).

liability for unauthorized use of her credit card or credit card data.[639] Regulation Z's billing error resolution procedure[640] allows the consumer to contest a billing statement that reflects a charge for property or services not accepted by the consumer *or not delivered to the consumer as agreed*.[641] If this error is ascertained in the resolution procedure, the card issuer has to credit the consumer's account with the disputed amount.[642] One important consequence of this procedure is that it protects the consumer against being charged for goods or services that she never received or that were otherwise not delivered or performed as agreed. The procedure affords cheap redress to consumers who did not get what they paid for with their credit card.

### b) Chargebacks as a General Enforcement Model

The chargeback mechanism in U.S. credit card regulation is unique in two regards. It does not exist anywhere else in the world,[643] and even in the U.S. it does not apply to any other payment system. While the credit card regulations in most countries are similar regarding *unauthorized* payments, they are not in regard to transactions that go wrong *after* a payment has actually been

---

[639] *See supra* note 64 and accompanying text.

[640] *See supra* note 638, § 226.13. *See generally* LAWRENCE, *supra* note 67, at 526 (giving an overview on the billing error resolution procedure).

[641] *See supra* note 638, § 226.13(a)(3).

[642] *See id.* § 226.13(e)(1). The card issuer will generally pass its loss on to the merchant. *See supra* note 67 and accompanying text.

[643] *See* OECD, *Consumer Redress in the Global Marketplace: Chargebacks*, OCDE/GD(96)142, at 54-71, available online at <http://www.oecd.org//dsti/sti/it/consumer/e_96-142.pdf> [hereinafter

authorized by the consumer. Under the laws of other countries the card issuer does not pay any attention to defenses or claims of the cardholder stemming from her transaction with the merchant.[644] The cardholder will be charged when she authorized the payment. Whether she actually receives the goods she paid for or not is a problem to be resolved solely among her and the merchant. In this regard the laws are thus much less favorable to consumers than in the U.S.

The crucial middle position of payment intermediaries and their ability to guarantee effective and cheap redress to consumers and thereby foster consumer reliance, however, suggests that the adoption of mandatory chargeback regimes in cases of problems in the *underlying transaction* between the consumer and the merchant might generally be advisable from a policy perspective.[645]

Payment intermediaries are typically linked to both parties directly or indirectly through contracts or a chain of contracts, which gives them an opportunity to verify the identity and locate the whereabouts of both the merchant and the consumer. They have a significant leverage on the merchant, because it is the

---

OECD, *Chargebacks*] (providing an overview on the situation regarding chargeback regimes in the OECD member countries).

[644] The same is true for voluntary industry codes. *See id.* at 7 ("Chargebacks are more likely in cases of fraud or billing disputes. Some card companies still appear reluctant to offer chargebacks in cases of dispute about misrepresentation or nonconformance of goods.").

[645] This question is also raised by Rothchild, *supra* note 31, at 977 ("The establishment of a comprehensive international chargeback regime will greatly enhance consumers' willingness to enter into online transactions with distant sellers, and will provide consumers with an avenue of redress."); ACCC, *Enforcement Challenge, supra* note 28, at 25; Heckman, *supra* note 113, at 2.8 (pointing to existing intervention of credit card companies as a possible model for new

only party the merchant—if it wants to get its money, which is typically the ultimate goal for both honest and fraudulent merchants—really depends on. The payment provider can use this leverage to contractually provide for a right to charge back amounts to the merchant that it (the merchant) is not entitled to keep.[646] Ultimately, the payment provider could use its leverage to terminate their service to specific merchants, which would effectively cut these merchants off the revenue stream and would induce them to comply in the first place. On the other hand payment intermediaries are in a position that allows them to afford consumers quick and cheap redress by simply reversing the payment transaction and recrediting the disputed amount back to their account. Such chargeback mechanisms can effectively mitigate the risk of prior performance.[647] This risk is the reason for consumers' vulnerability in distance transactions and the main factor that leads to a need for trust and reliance in this context. Payment providers thus are well suited to step in and fix things for the consumer if they go wrong. They could provide effective enforcement and serve as a basis for consumer *reliance* and avoid the high information costs connected with attempts to enhance consumer *trust*.

On the other hand, the risks of misuse of chargeback mechanisms by consumers seem manageable. In the case of tangible products merchants can use delivery

---

intermediaries facilitating consumer redress). For a comprehensive summary of a respective round-table discussion see OECD, *Chargebacks, supra* note 643.

[646] Which is the common procedure in cases of unauthorized use of credit card data. *See supra* note 67 and accompanying text.

[647] *See supra* note 93.

services providing a delivery confirmation to prevent consumers from falsely alleging that the merchandise has never arrived. The merchant could provide this confirmation to prevent a chargeback. In the case of digital products or services that are delivered online the problem does not seem to exist. The merchant can simply transmit the data again. The consumer, should she in fact already have received the data, could always make an additional copy anyway. So re-sending the data does not hurt the merchant—and the consumer would actually have no incentive to falsely state that she has not received anything. Regarding merchandise that did arrive but allegedly is defective, things are a little more complicated since a delivery confirmation will normally not give any information about the condition of the goods that have been delivered. Here the chargeback could be afforded under the condition that the consumer provides a confirmation that the goods have been returned to the merchant.

In any event, a chargeback would not preclude the merchant from contesting the consumer's allegations in court. Chargebacks in effect do nothing else than shifting the burden of having to take legal action in the event of a dispute[648] back to the merchant,[649] which arguably is the party that is better equipped to bear that burden in the first place. Since the threat of bringing suit by a merchant is much more credible than the same threat by a consumer, consumers will generally be discouraged from misusing chargeback mechanisms to cheat a merchant.

---

[648] Which has been allocated to the consumer by her having to perform in advance, *see supra* note 99 and accompanying text.

[649] ACCC, *Enforcement Challenge, supra* note 28, at 25 ("the burden is taken off the consumer to initiate lawsuits and placed on the merchant").

# IV. CONCLUSIONS

Consumers will not engage in impersonal exchange unless they either *trust* the merchant they are dealing with and believe that everything will go alright or they can comfortably *rely* on a third party to effectively afford them redress if things go wrong. Trust and reliance, which are to a large extent grounded on expected compliance and effective enforcement, are two distinct components of consumer confidence. This paper has discussed why traditional bases for trust and reliance are no longer effective in the electronic marketplace. It argues that new institutions will emerge to enhance trust and reliance, namely information intermediaries and payment intermediaries, respectively. Of these two options, reliance mechanisms that can guarantee cheap and effective enforcement of consumer rights ultimately appear to be the more efficient approach to overcome the lack of consumer confidence.

The paper has shown that some of these reliance mechanisms have developed in the market and it has pointed out the crucial role of payment intermediaries in *every* online transaction. From a policy perspective it has suggested to leverage this role and consider addressing payment intermediaries by introducing comprehensive chargeback regimes that could guarantee effective consumer redress if something goes wrong in the transaction between merchant and consumer.

One puzzle, however, seems to remain unsolved. A chargeback regime similar to the proposal made in this paper in fact does exist in U.S. credit card regulation. If

that is so, however, why is the lack of consumer confidence not a purely non-U.S. problem? There are two answers to this question. First, electronic commerce is doing significantly better in the U.S. than in other parts of the world.[650] This paper asserts that this difference is partly due to the fact that U.S. consumers do have greater confidence in shopping online because of the more favorable legislative framework for credit card payments. Second, consumers' fear of being defrauded by an unknown merchant is not the only inhibitor of electronic commerce. The other two major concerns of consumers are security and privacy. These two concerns prevent a significant number of users *to use their credit card online at all*. Thus, while the credit card chargeback regime could in fact give consumers greater confidence in regard of consumers' fears of fraud, the other two concerns prevent consumers from using their credit card and benefiting from the former. The three issues therefore are interdependent and need to be addressed as such. An important step in addressing the issues is consumer education. At least consumers' fears of being liable for an unauthorized use of their credit card data after a security breach are, from a legal point of view, irrationally exaggerated[651] and presumably due to a lack of knowledge about the legal risk allocation, which is in effect extremely favorable to consumers. The privacy issues, being the remaining major obstacle to consumer confidence, need to addressed aggressively by the private and the public sector.

---

[650] *See supra* note 12.

[651] *See supra* note 77.

As to the obstacles to consumer confidence that have stood in the center of this paper, however, chargeback mechanisms appear to be a powerful remedy. "[C]onsumers must have confidence ... that they will get what they pay for, and that recourse or redress will be available if they do not."[652] Chargeback mechanisms appear to be a tool that can guarantee the latter. Therefore the paper argues that they are an approach worth pursuing in order to overcome "the global enforcement challenge" presented by the new online marketplace.

---

[652] *See supra* note 15.

# BIBLIOGRAPHY


- Alliance for Global Business, *A Global Action Plan for Electronic Commerce: Prepared by Business with Recommendations for Governments* (2d ed. 1999), available online at <http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/bizac_e.pdf> (identical with OECD Doc. SG/EC(99)6)
- American Institute of Certified Public Accountants, Inc. & Canadian Institute of Chartered Accountants, *Web Trust Principles and Criteria for Business-to-Consumer Electronic Commerce* (Oct. 15, 1999) <http://www.aicpa.org/webtrust/princritb.htm>
- Sarah Andrews & Andrew Shen, Electronic Privacy Information Center, *Public Comment on Barriers to Electronic Commerce: U.S. Department of Commerce—Office of the General Counsel; Laws or Regulations Posing Barriers to Electronic Commerce* (Mar. 17, 2000) <http://www.epic.org/privacy/internet/Barriers_to_E-commerce.html>
- KENNETH J. ARROW, THE LIMITS OF ORGANIZATION (1974)
- Australian Competition & Consumer Commission, *The Global Enforcement Challenge: Enforcement of consumer protection laws in a global marketplace* (Aug. 1997), available online at <http://www.accc.gov.au/docs/global/front.htm>
- Neil W. Averitt & Robert H. Lande, *Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law*, 65 ANTITRUST L.J. 713 (1997)

- ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984)
- Reinhard Bachmann, *Conclusion: Trust—Conceptual Aspects of a Complex Phenomenon, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 298 (Christel Lane & Reinhard Bachmann eds., 1998)
- ANNETTE BAIER, POSTURES OF THE MIND (1995)
- Annette Baier, *Trust and Antitrust*, 96 ETHICS 231 (1986)
- DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW (1994)
- STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST (1998)
- BERNHARD BARBER, THE LOGIC AND LIMITS OF TRUST (1983)
- John Perry Barlow, *A Cyberspace Independence Declaration* (Feb. 9, 1996) <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>
- Jay B. Barney & Mark H. Hansen, *Trustworthiness as a Source of Competitive Advantage*, 15 STRATEGIC MGMT. J. 175 (1994)
- DANIEL J. BARRETT, BANDITS ON THE INFORMATION SUPERHIGHWAY (1996)
- BBBOnline, *Reliability Program* (visited Aug. 17, 00) <http://www.bbbonline.com/businesses/reliability/index.html>
- BBBOnline, *Standards for BBBOnline Reliability Program Participation* (visited Aug. 17, 00) <http://www.bbbonline.com/businesses/reliability/standards.html>

- Lucian Arye Bebchuk, *A New Theory Concerning the Credibility and Success of Threats to Sue*, 25 J. LEGAL STUD. 1 (1996)
- Lucian Arye Bebchuk & Howard F. Chang, *An Analysis of Fee Shifting Based on the Margin of Victory: On Frivolous Suits, Meritorious Suits, and the Role of Rule 11*, 25 J. LEGAL STUD. 371 (1996)
- Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. LEGAL STUD. 115 (1992)
- Lisa Bernstein, *Private Commercial Law, in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 108 (Peter Newman ed., 1998)
- Jonathan D. Bick, *Why Should the Internet be Any Different?*, 19 PACE L. REV. 41 (1998)
- Bizrate.com, *About BizRate.com—Store Ratings* (visited Aug. 17, 00) <http://www.bizrate.com/inside/ratings.xpml>
- Louis H. Bluhm, *Trust, Terrorism, and Technology*, 6 J. BUS. ETHICS 333 (1987)
- GARY B. BORN, , INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS (3d ed. 1996)
- George G. Brenkert, *Trust, Morality, and International Business, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 272 (Christel Lane & Reinhard Bachmann eds., 1998)
- Mike Brunker, *Data thief threatens to strike again*, ZDNet UK (Jan. 12, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12574.html>

- Bundesrechtsanwaltskammer [German Bar Association], *German Attorney's Fees* (visited Aug. 17, 00) <http://www.brak.de/aktuelles/3Dgebo-e.html>
- MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY (1996)
- Bruce Chapman, *Trust, Economic Rationality, and the Corporate Fiduciary*, 43 U. TORONTO L.J. 547 (1993)
- David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373 (1990)
- Cheskin Research & Studio Archetype/Sapient, *eCommerce Trust Study* (Jan. 1999), available at <http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf>
- David Church et al., *Recent Developments Regarding U.S. and EU Regulation of Electronic Commerce*, 33 INT'L LAW. 347 (1999)
- Charles Clark, *The Answer to the Machine is in the Machine, in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 139 (P. Bernt Hugenholtz ed., 1996)
- WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), available at <http://www.ecommerce.gov/framewrk.htm>
- RALPH C. CLONTZ, JR., TRUTH-IN-LENDING MANUAL (Update No. 3, 1997).
- RONALD H. COASE, THE FIRM, THE MARKET, AND THE LAW (1988)
- Comment, *Civil RICO and Its Application to "Garden Variety" Fraud Within the Sixth Circuit*, 13 N. KY. L. REV. 463 (1987)

- Comment, *What Have They Done to Civil RICO: The Supreme Court Takes the Racketeering Requirement Out of Racketeering*, 35 AM. U. L. REV. 821 (1986)
- Consumer Reports Online, *e-Ratings Online Shopping Guide* (visited Aug. 17, 00) <http://www.consumerreports.org/Special/Samples/Reports/0001erat.htm>
- Consumers International, *Consumers@shopping: An international comparative study of electronic commerce* (1999), available online at <http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf>
- Consumers International, Consumers@shopping: *An international comparative study of electronic commerce* (Sept. 1999) <http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf>
- Robert D. Cooter & Daniel L. Rubinfeld, *Economic Analysis of Legal Disputes and Their Resolution*, 27 J. ECON. LIT. 1067 (1989)
- Robert D. Cooter, *Structural Adjudication and the New Law Merchant: A Model of Decentralized Law*, 14 INT'L REV. L. & ECON. 215 (1994)
- CPA WebTrust, *It's a Matter of Trust* (visited Aug. 17, 00) <http://www.cpawebtrust.com/consumer/index.html>
- Pavel Curtis, *MUDding: Social Phenomena in Text-based Virtual Realities, in* HIGH NOON ON THE ELECTRONIC FRONTIER 347 (Peter Ludlow ed., 1996)
- Partha Dasgupta, *Trust as a Commodity, in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 49 (Diego Gambetta ed., 1988)

- Simon Deakin & Frank Wilkinson, *Contract Law and the Economics of Interorganizational Trust, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 146 (Christel Lane & Reinhard Bachmann eds., 1998)
- John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT. L.J. 207 (1997)
- Julian Dibbell, *A Rape in Cyberspace; or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society, in* HIGH NOON ON THE ELECTRONIC FRONTIER 375 (Peter Ludlow ed., 1996)
- Frank Diedrich, *Internationales Einheitsrecht—Internationalisierung der Rechtswissenschaft?, in* JAHRBUCH JUNGER ZIVILRECHTSWISSENSCHAFTLER 1998: VERNETZTE WELT—GLOBALES RECHT 45 (Martin Immenhauser & Jürg Wichtermann eds., 1999)
- Angela Drolte, *U.S. Consumers Advocate Doubts Effectiveness of Industry-Initiated Online Privacy Policies*, 2 ELECTRONIC COMMERCE & L. REP. (BNA) 601 (June 13, 1997)
- Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 Jurimetrics J. 1 (1994)
- Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996)

- Ebay, *The Feedback Forum* (visited Aug. 17, 00) <http://pages.ebay.com/services/forum/feedback.html>
- ROBERT C. ELLICKSON, ORDER WITHOUT LAW (1990)
- European Commission, Health and Consumer Protection, *Access to Justice* (visited Aug. 17, 00) <http://www.europa.eu.int/comm/dg24/policy/developments/acce_just/index_en.html>
- European Commission, *Working Paper on Enforcement of European Consumer Legislation* 14 (visited Aug. 17, 00) <http://www.europa.eu.int/comm/dg24/policy/developments/enfo/enfo01_en.pdf>
- *A European Initiative in Electronic Commerce*, COM(97)157 final
- Ellen M. Faro, Note, *Telemarketing Credit Card Fraud: Is RICO one Answer?*, 1990 U. ILL. L. REV. 675
- Matthew J. Feeley, *EU Internet Regulation Policy: The Rise of Self-Regulation*, 22 B.C. INT'L & COMP. L. REV. 159 (1999)
- BIRGIT FELDTMANN ET AL., THE COST OF LEGAL OBSTACLES TO THE DISADVANTAGE OF CONSUMERS IN THE SINGLE MARKET, A REPORT FOR THE EUROPEAN COMMISSION DG XXIV – CONSUMER POLICY AND CONSUMER HEALTH PROTECTION (1998)
- Todd H. Flaming, *The Rules of Cyberspace: Informal Law in a New Jurisdiction*, 85 ILL. B.J. 174 (1997)

- Forrester Research, Inc., Press Release, *eCommerce Could Be Hindered By Order Fulfillment Chaos* (Aug. 26, 1999) <http://www.forrester.com/ER/Press/Release/0,1769,160,FF.html>
- *Fraud continues to deter e-shoppers*, IT-Analysis.com (Nov. 22, 1999) <http://www.it-analysis.com/99-11-22-2.html>
- Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996)
- Federal Trade Commission, *150 Organizations in 28 Countries Tackle Internet Fraud* (March 23, 2000) <http://www.ftc.gov/opa/2000/03/rich.htm>
- Federal Trade Commission, Staff Report, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech Global Marketplace* (May 1996) <http://www.ftc.gov/opp/global/report/gc_v2.pdf>
- Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* (April 1998) <http://www.ftc.gov/ogc/brfovrvw.htm>
- Federal Trade Commission, *Commission Enforcement Actions Involving the Internet and Online Services* (Dec. 15, 1999) <http://www.ftc.gov/opa/1999/9912/case121599.pdf>
- Federal Trade Commission, Bureau of Consumer Protection, *Complaint Form* (last modified Feb. 18, 2000) <https://www.ftc.gov/ftc/complaint.htm>

- Federal Trade Commission, Report, *Fighting Consumer Fraud: The Challenge and the Campaign* (Jan. 1997) <http://www.ftc.gov/reports/Fraud/index.htm>
- Federal Trade Commission, Report, *Fighting Consumer Fraud: New Tools of the Trade* (April 1998) <http://www.ftc.gov/reports/fraud97/fraud97.pdf>
- Federal Trade Commission, Report, *The FTC's First Five Years Protecting Consumers Online* (Dec. 1999) <http://www.ftc.gov/os/1999/9912/fiveyearreport.pdf>
- Federal Trade Commission, *Statutes Enforced or Administered by the Commission* (last modified July 15, 1999) <http://www.ftc.gov/ogc/stats.htm>
- Drew Fudenberg & Eric Maskin, *The Folk Theorem in Repeated Games With Discounting or With Incomplete Information*, 54 ECONOMETRICA 533 (1986)
- FRANCIS FUKUYAMA, TRUST (1995).
- Nancy R. Furnari, *Are Traditional Agency Principles Effective for Internet Transactions, Given the Lack of Personal Interaction?*, 63 ALB. L. REV. 537 (1999)
- Randy Gainer, *Allocating the Risk of Loss for Bank Card Fraud on the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 39 (1996)
- Llewellyin Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475 (1997)

- Global Business Dialogue on Electronic Commerce (GBDe), *The Paris Recommendations* (Sep. 13, 1999) (visited Aug. 17, 00) <http://www.gbd.org/conference/recommendations.html>
- Global Information Networks, Ministerial Conference Bonn 6-8 July 1997, *Ministerial Declaration* (visited Aug. 17, 00) <http://www2.echo.lu/bonn/final.htm>
- Bernd Goecke, *Re: Kreditkarten im Internet* (Feb. 18, 2000), posted to netlaw-l@listserv.gmd.de, available online in the list's archive at <http://www.listserv.gmd.de/htbin/wa.exe?A2=ind0002&L=netlaw-l&F=&S=&P=23268>
- Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998)
- John P. Gould, *The Economics of Legal Conflicts*, 2 J. LEGAL STUD. 279 (1973)
- TRUDY GOVIER, DILEMMAS OF TRUST (1998)
- TRUDY GOVIER, SOCIAL TRUST AND HUMAN COMMUNITIES (1997)
- Fred M. Greguras et al., *Software Marketing, Licensing and Distribution in Cyberspace*, 1 CYBERSPACE LAW. 4 (1996)
- Avner Greif, *Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition*, 83 AM. ECON. REV. 525 (1993)
- Avner Greif et al., *Coordination, Commitment, and Enforcement: The Case of the Merchant Guild*, 102 J. POL. ECON. 745 (1994)

- Avner Greif, *Informal Contract Enforcement, in* 2 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 287 (Peter Newman ed., 1998)
- Avner Greif, *Institutions and International Trade: Lessons from the Commercial Revolution*, 82 AEA PAPERS & PROC. 128 (1992)
- David L. Gripman, *Electronic Document Verification: A Primer on the Technology Behind Digital Signatures*, 17 J. MARSHALL J. COMPUTER & INFO. L. 769 (1999)
- *The growing threat of internet fraud*, BBC News (Nov. 19, 1999) <http://news.bbc.co.uk/hi/english/business/your_money/newsid_526000/526709.stm>
- Connie Guglielmo, *Consumers reluctant to rely on Net*, ZDNet UK (Dec. 13, 1999) <http://www.zdnet.co.uk/news/1999/49/ns-12127.html>
- Saul Hansell, *Toys 'R' Us Falls Behind on Shipping*, N.Y. TIMES, Dec. 23, 1999, at <http://www.nytimes.com/library/tech/99/12/biztech/articles/23toy.html>
- Russell Hardin, *Trust, in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 623 (Peter Newman ed., 1998)
- Cynthia Hardy et al., *Distinguishing Trust and Power in Interorganizational Relations: Forms and Façades of Trust*, *in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 64 (Christel Lane & Reinhard Bachmann eds., 1998)
- Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993 (1994)

- HENRY M. HART, JR. & ALBERT M. SACKS, THE LEGAL PROCESS (1994)
- Carey Heckman, *Gateways to the Global Market: Consumers and Electronic Commerce* (visited Aug. 17, 00) <http://www-techlaw.stanford.edu/pages/OECDBack.html>
- Virginia Held, *On the Meaning of Trust*, 78 ETHICS 156 (1968)
- HIGH NOON ON THE ELECTRONIC FRONTIER (Peter Ludlow ed., 1996)
- DOUGLAS R. HOFSTADTER, METAMAGICAL THEMAS: QUESTING FOR THE ESSENCE OF MIND AND PATTERN (1985)
- MARTIN HOLLIS, TRUST WITHIN REASON (1998)
- John Humphrey, *Trust and the Transformation of Supplier Relations in Indian Industry, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 214 (Christel Lane & Reinhard Bachmann eds., 1998)
- WILLIAM HAROLD HUTT, ECONOMISTS AND THE PUBLIC (1936)
- David R. Johnson & David Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996)
- Maryann Jones Thompson, *Spotlight: Why E-commerce Forecasters Don't Get It "Right"*, The Standard (Mar. 1, 1999) <http://www.thestandard.com/research/metrics/display/0,2799,9881,00.html>
- Maryann Jones Thompson, *E-commerce Spotlight: Building Trust Online*, THE STANDARD (Jan. 25, 1999) <http://www.thestandard.com/research/metrics/display/0,2799,9928,00.html>

- Jupiter Communications, Press Release, *64 Percent of Online Consumers are Unlikely to Trust a Web Site* (Aug. 17, 1999) <http://www.jup.com/company/pressrelease.jsp?doc=pr990817>
- Carl S. Kaplan, *On the Web, It's Buyer Beware. But Where?*, N.Y. TIMES, CYBER LAW JOURNAL (March 26, 1999) <http://www.nytimes.com/library/tech/99/03/cyber/cyberlaw/26law.html>
- Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. 675 (1999)
- Louise Kehoe, *A Valentine's Day fiasco,* FT.com (Feb. 20, 2000) <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT4KVRU4X4C>
- Jake Kirchner, *Forget having privacy on the Net*, ZDNet News (March 22, 2000) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2472006,00.html>
- Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615 (1981)
- Will Knight, *Every e-commerce site's nightmare as hacker gets nasty with credit card details*, ZDNet UK (Jan. 12, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12576.html>
- Amy Knoll, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275 (1996)

- Helmut Köhler, *Die Rechte des Verbrauchers beim Teleshopping (TV-Shopping, Internet-Shopping*), 1998 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 185
- David M. Kreps et al., *Rational Cooperation in the Finitely Repeated Prisoners' Dilemma*, J. ECON. THEORY 245 (1982)
- William M. Landes, *An Economic Analysis of the Courts*, 14 J. LAW & ECON. 61 (1971)
- Christel Lane, *Introduction: Theories and Issues in the Study of Trust, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 1 (Christel Lane & Reinhard Bachmann eds., 1998)
- LARY LAWRENCE, AN INTRODUCTION TO PAYMENT SYSTEMS (1997).
- Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839 (1999)
- Dieter Leipold, *Limiting Costs for Better Access to Justice: The German Approach*, *in* REFORM OF CIVIL PROCEDURE 265, 266-275 (A.A.S. Zuckermann & Ross Cranston eds., 1995)
- LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999)
- Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1402 (1996)
- Linda Leung, *Five per cent of all online transactions are fraudulent*, vnunet.com (Nov. 24, 1999) <http://www.vnunet.com/News/103736>

- *Like stealing credit cards from babies*, ZDNet UK (Jan. 13, 2000) <http://www.zdnet.co.uk/news/2000/1/ns-12608.html>
- Toni Logan, *Lights! Camera! Stock Options! Celebrities help ebusinesses build brand, but can star power substitute for an integrated marketing strategy?*, BUSINESS 2.0, April 2000, at 165
- Niklas Luhmann, *Familiarity, Confidence, Trust: Problems and Alternatives, in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 94 (Diego Gambetta ed., 1988)
- NIKLAS LUHMANN, TRUST AND POWER (1979)
- Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOC. REV. 55 (1963)
- MasterCard, *Shop Online: SET* (visited Aug. 17, 00) <http://www.mastercard.com/shoponline/set>
- Philipp J. Mause, *Winner Takes All: A Re-Examination of the Indemnity System*, 55 IOWA L. REV. 26 (1969)
- Roger C. Mayer et al., *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709 (1995)
- William S. Mayfield, *Consumer Protection*, 13 S.U. L. REV. 279 (1987)
- Eric J. McCarthy, *Networking in Cyberspace: Electronic Defamation and the Potential for International Forum Shopping*, 16 U. PA. J. INT'L BUS. L. 527 (1995)

- Dermot McGrath, *When 'E' Stands for Europe*, COMPUTERWORLD, Sept.6, 1999, at 52
- Paul R. Milgrom et al., *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs*, 2 ECON. & POL. 1 (1990)
- Fred H. Miller, *Consumers and the Code: The Search for the Proper Formula*, 75 WASH. U. L.Q. 187 (1997)
- John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAW. 403 (1998)
- Timothy J. Muris, *Economics and Consumer Protection*, 60 ANTITRUST L.J. 103 (1991)
- The National Advisory Council on Consumer Affairs (Australia), *Consumer Protection in Electronic Commerce* (April 1998), available online at <http://www.treasury.gov.au/publications/ConsumerAffairs/ElectronicCommercePublications/ConsumerProtectionInElectronicCommerce-PrinciplesAndKeyIssues/index.asp>
- Dan L. Nicewander, *Electronic Banking—Smart Cards, Cyberspace and the Internet*, 50 CONSUMER FIN. L.Q. REP. 22 (1996)
- Norman H. Nie & Lutz Erbring, Stanford Institute for the Quantitative Study of Society, *Internet and Society: A Preliminary Report* (Feb. 17, 2000) <http://www.stanford.edu/group/siqss/Press_Release/Preliminary_Report.pdf>

- DOUGLASS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE, AND ECONOMIC PERFORMANCE (1990)
- Note, *Civil RICO and "Garden Variety" Fraud—A Suggested Analysis*, 58 ST. JOHN'S L. REV. 93 (1983)
- Kathleen O'Toole, *Study takes early look at social consequences of Net use*, STANFORD REPORT [ONLINE] (Feb. 16, 2000) <http://www.stanford.edu/dept/news/report/news/february16/internetsurvey-216.html>
- OECD, *Business-to-Consumer Electronic Commerce: Survey of Status and Issues*, OCDE/GD(97)219, available at <http://www.oecd.org/dsti/sti/it/ec/prod/gd97219e.pdf>
- OECD, Directorate for Science, Technology and Industry, Committee on Consumer Policy, *Consumer Protection in the Electronic Marketplace*, DSTI/CP(98)13/FINAL (Dec. 22, 1998)
- OECD, *Consumer Redress in the Global Marketplace: Chargebacks*, OCDE/GD(96)142, available at <http://www.oecd.org//dsti/sti/it/consumer/e_96-142.pdf>
- OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on Indicators for the Information Society, *Defining and Measuring E-Commerce: A Status Report*, DSTI/ICCP/IIS(99)4/FINAL (Oct. 7, 1999)

- OECD, THE ECONOMIC AND SOCIAL IMPACT OF ELECTRONIC COMMERCE: PRELIMINARY FINDINGS AND RESEARCH AGENDA (1999)
- OECD, Directorate for Science, Technology and Industry, *OECD Forum on Electronic Commerce: Report on the Forum*, SG/EC(99)12 at 13 (Nov. 24, 1999), available at <http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/forum_report.pdf>
- OECD, Directorate for Science, Technology and Industry, *OECD Forum on Electronic Commerce: Report on the Forum, OECD, Paris, 12-13 October 1999*, SG/EC(99)12 (Nov. 24, 1999)
- OECD, Directorate for Science, Technology and Industry, Steering Committee for the Ottawa Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce", *A Global Action Plan for Electronic Commerce Prepared by Business With Recommendations From* [sic!] *Governments*, SG/EC(98)11/REV2 (Oct. 5, 1998), available at <http://www.oecd.org//dsti/sti/it/ec/prod/sgec_11e.pdf>
- OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on the Information Economy, *Measuring Electronic Commerce: International Trade in Software*, DSTI/ICCP/IE(98)3/FINAL (April 27, 1998)
- OECD, Committee for Information, Computer and Communications Policy, *Measuring Electronic Commerce*, OCDE/GD(97)185

- OECD, *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce* (Dec. 9, 1999) <http://www.oecd.org/dsti/sti/it/consumer/prod/CPGuidelines_final.pdf>
- OECD, Directorate for Science, Technology and Industry, Industry Committee, Working Party on Small and Medium-Sized Enterprises, *SMEs and Electronic Commerce*, DSTI/IND/PME(98)18/REV1 (Sept. 18, 1998), available at <http://www.oecd.org/dsti/sti/it/ec/prod/sme18e.pdf>
- Andersen Consulting, Press Release, *One Quarter of Attempted On-Line Holiday Purchases End in "No Sale"* (Dec. 20, 1999) <http://www.andersen.com/news/newsarchive/12.99/newsarchive_122099.html>
- Ernest T. Patrickis & Stephanie Heller, *The Government's Role in Electronic Commerce: A Review of the Clinton Administration's Framework on Global Electronic Commerce*, 18 ANN. REV. BANKING L. 325 (1999)
- Henry H. Perritt, Jr., *Townhall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413 (1997)
- Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349 (1993)
- Rufus Pichler, *Business-to-Consumer Electronic Commerce: The Economics of Litigation and Online Dispute Resolution* (Dec. 21, 1999) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies)

- Rufus Pichler, *The Directive 97/7/EC of the European Parliament and of the Council on the Protection of Consumers in Respect of Distance Contracts: Theoretical and Practical Impacts on Transatlantic Electronic Commerce* (Dec. 22, 1999) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies)
- Rufus Pichler, *Kreditkartenzahlung im Internet*, 1998 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 3234
- RUFUS PICHLER, RECHTSNATUR, RECHTSBEZIEHUNGEN UND ZIVILRECHTLICHE HAFTUNG BEIM ELEKTRONISCHEN ZAHLUNGSVERKEHR IM INTERNET (1998)
- Rufus Pichler, *Richtlinienvorschlag zu elektronischen Signaturen*, 1998 EUROPEAN LAW REPORTER 523
- Rufus Pichler, *Signaturrichtlinie*, 2000 EUROPEAN LAW REPORTER 75
- Stephen Craig Pirrong, *Self-Regulation of Private Organized Markets, in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 433 (Peter Newman ed., 1998)
- Robert Pitofsky, *Electronic Commerce and Beyond: Challenges of the New Digital Age* (Feb. 10, 2000) <http://www.ftc.gov/speeches/pitofsky/rpwilson2.htm>
- MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND ECONOMICS (2d ed. 1989)
- Mitchell Polinsky & Steven Shavell, *Legal Error, Litigation, and the Incentive to Obey the Law*, 5 J. L. ECON. & ORG. 99 (1989)

- Julia Porter Liebeskind & Amalya Lumerman Oliver, *From Handshake to Contract: Intellectual Property, Trust, and the Social Structure of Academic Research, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 118 (Christel Lane & Reinhard Bachmann eds., 1998)
- Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action*, 63 U. CHI. L. REV. 133 (1996)
- RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (5th ed. 1998)
- Richard A. Posner, *An Economic Approach to Legal Procedure and Judicial Administration*, 2 J. LEGAL STUD. 399 (1973)
- David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3 (June 1995) <http://warthog.cc.wm.edu/law/publications/jol/post.html>
- David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155 (1996)
- David G. Post, *The "Unsettled Paradox": The Internet, The State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521 (1998)
- David G. Post & David R. Johnson, Working Paper, *The New Civic Virtue of the Net: Lessons from Models of Complex Systems for the Governance of Cyberspace*, 1997 STAN. TECH. L. REV. (visited Aug. 17, 00) <http://stlr.stanford.edu/STLR/Working_Papers/97_Post_1/index.htm>
- PriceWaterhouseCoopers, *The BetterWeb Program* (visited Aug. 17, 00) <http://pwcbetterweb.com>

- PriceWaterhouseCoopers, *E-Business: A Matter of Trust* (1999) <http://www.e-business.pwcglobal.com/pdf/trust.pdf>
- Iain Ramsay, *Consumer Protection, in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 410 (Peter Newman ed., 1998)
- Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996)
- Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998)
- Andreas P. Reindl, *Consumer Contracts and European Community Law*, 75 WASH. U. L.Q. 627 (1997)
- HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993)
- Richard Richtmyer, *Amazon beats the Street: Online retailer sneaks past estimates; sees narrower operating losses*, CNNfn (April 26, 2000) <http://cnnfn.com/2000/04/26/technology/amazon>
- John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. 893 (1999)
- Edward L. Rubin, *The Nonjudicial Life of Contract: Beyond the Shadow of the Law*, 90 NW. U. L. REV. 107 (1995)
- Mari Sako, *Does Trust Improve Business Performance?, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 88 (Christel Lane & Reinhard Bachmann eds., 1998)

- HAIMO SCHACK, INTERNATIONALES ZIVILVERFAHRENSRECHT (2d ed. 1996)
- SET Secure Electronic Transactions LLC, *What is SET* (visited Aug. 17, 00) <http://www.setco.org/set.html>
- Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703 (1998)
- Steven Shavell, *The Social Versus The Private Incentive to Bring Suit in a Costly Legal System*, 11 J. LEGAL STUD. 333 (1982)
- Steven Shavell, *Suit, Settlement, and Trial: A Theoretical Analysis Under Alternative Methods for the Allocation of Legal Costs*, 11 J. LEGAL STUD. 55 (1982)
- Charles D. Siegal, *Rule Formation in Non-Hierarchical Systems*, 16 TEMP. ENVTL. L. & TECH. J. 173 (1998)
- Hebe R. Smythe, *Fighting Telemarketing Scams*, 17 HASTINGS COMM. & ENT. L.J. 347 (1994)
- David E. Sorkin, *Revocation of an Internet Domain Name for Violations of "Netiquette": Contractual and Constitutional Implications*, 15 J. MARSHALL J. COMPUTER & INFO. L. 587 (1997)
- Robert Spector, *Going for Broke*, BUSINESS 2.0, April 2000, at 256
- Stanford Institute for the Quantitative Study of Society, *Internet Study* (last modified Feb. 18, 2000) <http://www.stanford.edu/group/siqss/Press_Release/internetStudy.html>

- Robert F. Stankey, *Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers*, 6 COMMLAW CONSPECTUS 11 (1998)
- Tom Steinert-Threlkeld, *It's a new era—of economic blackmail*, ZDNet News (Feb. 9, 2000) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2435665,00.html>
- Stiftung Warentest, *Electronic commerce in Europe* (Sept. 1999) <http://www.europa.eu.int/comm/dg24/library/surveys/sur11_en.pdf>
- CLIFFORD STOLL, SILICON SNAKE OIL (1995)
- Bob Sullivan, *How to steal 2,500 credit cards*, ZDNet UK (Jan. 17, 2000) <http://www.zdnet.co.uk/news/2000/2/ns-12672.html> (
- Cass R. Sunstein, *From Consumer Sovereignty to Cost-Benefit Analysis: An Incompletely Theorized Agreement?*, 23 HARV. J.L. & PUB. POL'Y 203 (1999)
- Jörg Sydow, *Understanding the Constitution of Interorganizational Trust, in* TRUST WITHIN AND BETWEEN ORGANIZATIONS 31 (Christel Lane & Reinhard Bachmann eds., 1998)
- Symposium, *Cyberspace and Privacy—A New Legal Paradigm* 52 STAN. L. REV. (forthcoming 2000).
- Symposium, *Digital Signature and Electronic Document Verification*, 17 J. MARSHALL J. COMPUTER & INFO. L. 721 (1999)
- Joelle Tessler & Matt Marshall, *Online firms short on cash*, SAN JOSE MERCURY NEWS, April 1, 2000, A1

- Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561 (1998)
- TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH (Roderick M. Kramer & Tom R. Tyler eds., 1996)
- TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS (Diego Gambetta ed., 1988)
- TRUST WITHIN AND BETWEEN ORGANIZATIONS (Christel Lane & Reinhard Bachmann eds., 1998)
- Gordon Tullock, *The Prisoner's Dilemma and Mutual Trust*, 77 ETHICS 229 (1967)
- SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET (1995)
- U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998), available at <http://www.ecommerce.gov/EmergingDig.pdf>
- U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY II (1999), available at <http://www.ecommerce.gov/ede/ede2.pdf>
- United States Government, Electronic Commerce Policy, *Request for Public Comment on Legal Barriers to Electronic Commerce* (visited Aug. 17, 00) <http://osecnt13.osec.doc.gov/ecommerce/barriers.nsf>
- U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT (1998), available at <http://www.doc.gov/ecommerce/E-comm.pdf>

- U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, TOWARDS DIGITAL EQUALITY, SECOND ANNUAL REPORT (1999), available at <http://www.ecommerce.gov/ecomrce.pdf>
- VISA, *Internet Shopping: SET* (visited Aug. 17, 00) <http://www.visa.com/nt/ecomm/security/set.html>
- W. Kip Viscusi, *Using Warnings to Extend the Boundaries of Consumer Sovereignty*, 23 HARV. J.L. & PUB. POL'Y 211 (1999)
- Roland Vogl, *The EU—U.S. Privacy Debate* (May 2000) (unpublished manuscript) (on file with author and the Stanford Program in International Legal Studies)
- Jane Wakefield, *Online fraud warning to all e-commerce users*, ZDNet UK (Feb. 1, 2000) <http://www.zdnet.co.uk/news/2000/4/ns-13032.html>
- Jane Wakefield, *Media blamed for consumer online fears*, ZDNet UK (Aug. 18, 1999) <http://www.zdnet.co.uk/news/1999/32/ns-9370.html>
- Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995)
- JOHN O. WHITNEY, THE ECONOMICS OF TRUST: LIBERATING PROFITS AND RESTORING CORPORATE VITALITY (1995)
- OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM (1985)