

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/201754859>

A Framework for Studying the Problem of Trust in Online Settings

Chapter · January 2010

DOI: 10.4018/jdtis.2010070102

CITATIONS

0

READS

85

2 authors:



Guido Möllering

Universität Witten/Herdecke

95 PUBLICATIONS 1,620 CITATIONS

SEE PROFILE



Tina Guenther

5 PUBLICATIONS 23 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Project

Path Creating Networks [View project](#)

All content following this page was uploaded by [Guido Möllering](#) on 23 July 2014.

The user has requested enhancement of the downloaded file.

Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives

Dominika Latusek
Kozminski University, Poland

Alexandra Gerbasi
California State University, Northridge, USA

Information Science
REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Christine Bufton
Typesetter: Gregory Snader
Production Editor: Jamie Snavelly
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com/reference>

Copyright © 2010 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Trust and technology in a ubiquitous modern environment : theoretical and methodological perspectives / Dominika Latusek and Alexandra Gerbasi, editors. p. cm.

Includes bibliographical references and index.

Summary: "This book brings together scholars with significantly different backgrounds who share interests in the interplay between trust and technology, presenting novel theoretical perspectives on the topics of trust and technology, as well as some empirical investigations into the trust-building, trust-repairing, and trust-destroying practices in the context of technology"- Provided by publisher.

ISBN 978-1-61520-901-9 (hbk.) -- ISBN 978-1-61520-902-6 (ebook) 1. Technology--Psychological aspects. 2. Information technology--Psychological aspects. 3. Human-computer interaction--Psychological aspects. 4. Trust. I. Latusek, Dominika, 1981- II. Gerbasi, Alexandra, 1976- T49.5.T78 2010
303.48'3--dc22

2009040710

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 2

A Framework for Studying the Problem of Trust in Online Settings

Tina Guenther

Lecturer in Sociology, Founder and Author of Sozlog, Germany

Guido Möllering

Max Planck Institute for the Study of Societies, Germany

ABSTRACT

The chapter contributes to the conceptual foundations of research on trust in online settings by introducing a framework of the preconditions and constitutive elements of trust. Moving beyond simplistic, narrow, and vague applications of the notion of trust, researchers are enabled by this framework to recognize when trust is relevant and to address a broader range of elements and processes involved in the social constitution of trust. By way of illustration and differentiation, the authors discuss trust issues in online marketplaces and online communities in greater detail. An important message from the chapter is that the problem of trust does not only occur in specific activities on a particular website but, more importantly, through the interconnectedness of the websites used and the development of complex online biographies. Accordingly, the authors advocate research methods that are not only well-grounded conceptually but also geared praxeologically toward the actual experience and enactment of trust.

INTRODUCTION

The possibilities for entering into social relationships via digital technologies such as the internet have undoubtedly multiplied since the beginning of the 21st century. If relationships established ‘online’ involve uncertainty and vulnerability just like ‘offline’ relationships, we need to take a close look at online trust. We conceptualize ‘online trust’

broadly as the social accomplishment of having positive mutual expectations in an online setting which may still be disappointed and abused. More importantly, we are concerned in this chapter with the fact that the ‘online world’ is, of course, not separate from offline reality, meaning in particular that any harm – as well as any good – done on the internet will mostly have offline consequences, too. This is the case, at least, in social relationships that are technologically mediated but ultimately connecting human actors.

DOI: 10.4018/978-1-61520-901-9.ch002

Our chapter contributes to a better understanding of online trust by outlining a framework that will enable researchers to assess and analyze more thoroughly, if and how trust is an issue in online settings. After giving some background considerations that motivate our chapter, we will discuss the preconditions for trust's relevance. This is followed by a description of the different elements involved in the constitution of trust and how they play out in online settings. We then discuss the implications of our framework, with particular emphasis on the methodological requirements and opportunities for empirical work in this area. In the conclusion, we highlight the value of a sound conceptual grounding of trust instead of invoking it too loosely in research on online relationships.

BACKGROUND

What is commonly called “Web 2.0” and also the “Social Web” – indicating already a new quality of online activities – comprises a wide spectrum of ideas, utopias, and business models. We can distinguish developments in technology, civil society, modes of production, and entrepreneurship that together and in interaction with each other make up the new possibilities of “Web 2.0”.

First, in terms of technology, there are countless new applications such as weblogs, wiki webs, instant messaging, podcasts, RSS, social networking sites, and many more. The new technologies are designed to enable mass user participation and flexible reorganization of applications by users who create and recombine content, code, and metadata (Bruns, 2007; Guenther & Schmidt, 2008; Schmidt, 2006). Second, with this technological empowerment, “Web 2.0” can also denote an optimistic vision of a new civil society and the idea of a neo-Habermasian global public sphere of open discourse where critical discussions are possible, unconventional views can be expressed freely and the power of the state is counter-balanced (see Habermas, [1962]1989).

When the barriers to participation in new media are lowered, new arenas for exchanging information and opinions can emerge.

Third, the mode of production associated with “Web 2.0” is supposedly collaborative, heterarchical, and non-profit seeking. The content, code, and metadata going into such ‘open source’ products can challenge the proprietary solutions from the earlier days of the digital age (Benkler, 2006; Lessig, 2004). Fourth, it must be strongly emphasized, though, that the new opportunities are also part of a capitalist project that drives business and entrepreneurship ranging from e-commerce to a wealth of services and products offered by profit-seeking firms and individuals who use, maintain, or enhance the new technologies. It is by becoming more dynamic, integrative, interactive, and recombinant that the world of online media has entered into a new generation without a complete break from the internet of the 1990s.

The downside of increased connectedness is increased exposure. A highly dynamic world also carries higher uncertainty about the future. This makes trust a salient issue. The threats are well-documented by media reports, both online and offline, on crimes, privacy violations, and harassments made possible by the new digital media. Younger people are apparently less worried – though not less affected – by this, but middle-aged and older people are rather cautious, reluctant, and distrusting in their internet usage (Eimeren & Frees, 2008; PEW, 2005, 2008). It is important, though, to analyze clearly whether users merely see the possibility that nasty things can happen or whether they truly struggle to build and maintain trustful relationships with other users of online media. This is a complex matter because – as we will explore in this chapter – different realms of the online world as well as the online and offline worlds become increasingly interconnected, so that risks can spill over and grow to incalculable proportions. This brings trust into the picture even more.

Prior research has clearly recognized online trust as an issue, but tends to address it rather narrowly, focusing on security concerns to do with a particular kind of website, auctioning platform, e-commerce service, or social networking community (see Grabner-Kräuter & Kaluscha, 2003). We are missing a deeper analysis of the trust relationships involved, if any, and of the trust problems resulting from the use of multiple online services that may be rather harmless individually but can become dangerous when the various traces left by users are connected. Most studies on e-commerce in management, marketing, and organization capture only small parts of the overall problem (Belanger, Hiller & Smith 2002; McKnight & Chervany, 2002; McKnight et al., 2002; PEW, 2008; Shankar et al., 2002, 2003). Some work focuses just on the design of user interfaces (Brinkmann & Seifert, 2001; Gefen et al. 2003). Other authors broaden the picture by studying the effects of links between websites (Stewart, 2003) or the reputation systems that, ultimately, build on links between transactions and histories of user ratings (Bolton et al., 2004, 2008; Maztat, 2009). A different strand of research is concerned with privacy and surveillance issues, which comes closer to the broader picture that we look for, but usually portrays users in a rather passive role (Diaz, 2008; Hess, 2008; Zimmer, 2008).

Moreover, a fairly detailed study on trust in online communities by Thiedeke (2007) emphasizes the limitations of trust as a mechanism of complexity reduction and falls back on the maxim of “*Trust, but test!*” – i.e. the superiority of control over trust, which is a very common conclusion in research on online interaction. This view can be challenged, first, on the basis of research on the limited substitutability of trust and control, meaning that both are needed (Das & Teng, 1998; Long & Sitkin, 2006; Möllering, 2005) and, second, because it wrongly assumes that the online world can be clearly contained, e.g. by anonymity, so that none of the risks will spill over into the much less controllable offline world.

In working towards a deeper understanding of the problem of trust in online settings, we need to be clear under which conditions trust becomes relevant and we need to show how these preconditions apply in different online settings, for example internet-based markets and social networking sites. We address these points in the next section.

PRECONDITIONS OF THE RELEVANCE OF TRUST IN ONLINE SETTINGS

Defining and Delineating Trust

Mayer et al. (1995) propose that “trust is the willingness of a party to be vulnerable to the action of another party based on an expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (p. 712). Rousseau et al. (1998) define trust as a “psychological state comprising the intention to accept vulnerability based upon positive expectations or behavior of another” (p. 395). These definitions complement each other. They identify positive expectations in spite of vulnerability and uncertainty as the essential characteristic of trust.

Trust requires that at least two actors are involved (Baier, 1986), a trustor and a trustee, but these actors do not have to be persons. We follow the literature in allowing for impersonal trust and trust in systems, as long as it is meaningful to attribute actions, intentions, and social relations to the entities involved (see McKnight & Chervany, 2002; Shapiro, 1987). Hence it makes sense to speak of trust in relation to a service provider, online community, or the general internet public under these conditions. Moreover, relationships may be structured in such a way that actors are trustors and trustees at the same time, either to each other in a dyad or to third parties in chains and networks of relationships. When trust is invoked, though, it is necessary to be as precise

as possible about which actors are involved and in what kind of relationship they stand to each other. Actually, one of the practical issues of trust online is that the actors themselves often do not know who the others (really) are and what their networks of social relationships look like.

All the more, it is a precondition for trust's relevance that the actors we are interested in form more or less clear expectations about each other. Trust is a state of positive expectation, according to the definitions introduced above. If we cannot detect such expectations or if the actors we study are unable to form expectations, due to confusion or unfamiliarity, then trust is not applicable. More importantly, we should only speak of trusting expectations when they occur in the face of vulnerability and uncertainty (see Möllering, 2006). The social relationship between a trustor and a trustee is characterized by the fact that the trustor expects not to be harmed by the trustee, although the trustee is in a position to harm the trustor, and the trustor has neither perfect knowledge nor perfect control over the trustee's action. It is important to note that trust is the "willingness ... to be vulnerable" (Mayer et al. 1995, p. 712) but not "willingness to be hurt." Online settings that involve little or no mutual expectations, vulnerability, and uncertainty are probably unsuitable for an analysis of trust as a relevant issue.

If trust presumes at least two actors in a social relationship, then it is imperative to explore the agency and the embeddedness of these actors further. Trust requires agency in the sense that the trustor and the trustee must have a choice to grant or withhold trust and to honor or exploit trust respectively. At the same time, the choices they make have to be meaningful and this requires a social context in which the actors are embedded and which structures any situational manifestations of trust or distrust. If these requirements are fulfilled, then it makes sense to analyze in detail how trust unfolds as a matter of embedded agency.

The effort of defining and delineating trust is much less important as a scholarly exercise in the

interest of conceptual precision than as a practical task of establishing whether it makes sense to invoke trust as a relevant issue in a given online setting. We suggest actors, expectations, vulnerability, uncertainty, agency, and embeddedness as six preconditions that need to be considered. We contend that just being more explicit about these preconditions enhances our understanding of the role of trust in different settings already – including the likely insight that trust is less relevant in some settings than in others.

Relevance of Trust in Online Market Settings

In this subsection and the next we sketch the relevance of trust in two major settings, online marketplaces and social networking sites. We argue that the preconditions are generally fulfilled in both cases but in different ways. Looking at internet-based markets first, e-commerce takes place in the form of electronic markets, online shops, auction platforms, financial trading, private lending, and so on. There is broad agreement in the literature that online markets depend on trust to thrive (Belanger et al., 2002; Brinkmann & Seifert, 2001; Corritore et al., 2003; Gefen et al., 2003; Matzat, 2009; McKnight & Chervany, 2002; Bolton et al., 2004, 2008; Bolton & Ockenfels, 2006; Shankar et al., 2002, 2003; Wang & Emurian, 2005). Trust is required to enroll enough participants to a viable market and it is desired to reduce transaction costs caused by screening and other safeguarding mechanisms against opportunistic behavior by participants in the absence of trust and trustworthiness (e.g. Lorenz, 1988).

As a recent study shows for the United States (PEW, 2008), almost all internet users (93 percent) have engaged in economic activity online. On any day, more than a quarter of users engage in activities related to e-commerce such as searching for product information, making purchases or reservations, bidding in auctions, paying for downloads, or home banking including stock

trading. This suggests that participation in online market places is a routine matter for most internet users. However, the same study also finds that users worry about security online. According to the PEW results, some 43 percent of online users have been frustrated by the absence or intractability of relevant information online; 32 percent are confused by information provided; and 58 percent have experienced at least one of these worries in connection with online shopping. Providers recognize the importance of trust and are willing to make efforts to increase the trustworthiness of their platforms. Research and practice are often short-sighted, though, in that they frame the trust problem in terms of technology, interface design, incentives, or regulation devices for a specific marketplace. While all of these factors may come into play, trust goes deeper.

Despite some variance at the individual level, internet users generally worry not only about the successful completion of online transactions as such (e.g. the delivery of a book ordered online and the correct billing to a credit card), but also about the traces they leave online, personal information in particular. They know that providers often use and sometimes abuse such digital footprints for purposes that go beyond individual sales transactions. Users, in return, can share information about the seller and tell other users about their good or bad experiences by using online media outside the provider's platform. In other words, apparently transient market transactions give rise to social relations between users and providers that may effectively become permanent. And these relationships extend into the offline world, because users and providers usually cannot remain completely anonymous but need to validate their identities, for example, for billing and delivery purposes.

A closer look at the six preconditions for trust's relevance outlined above draws our attention, first of all, to the various actors involved in online market places. Around the transaction between a buyer and a seller who, as users, perform a transaction using an online platform,

other actors come in as providers of the platform, as firms offering financial or logistics services, as data storage specialists, or as regulators and certification agencies. As the relevant actors are identified, different trust issues may emerge in the various dyads. From the point of view of the buyer, for example, the seller is responsible for product quality, the internet provider for data security, the financial intermediary for payment, the logistics partner for timely delivery, and so on. What makes trust more difficult, both analytically and practically, is that the identity of all the actors involved in a transaction may actually be unknown and hard to ascertain.

These examples already suggest that many things can go wrong when using online marketplaces. The actors do form positive expectations about each other's intentions and behaviors, at least in the moment when they make the deal, but these expectations can be disappointed. Beneath the overall expectation of truthful and cooperative interaction, there are many specifics about who should do what and who ought to abstain from abusing their position opportunistically in one way or another. This gives each trust relationship a slightly different quality according to the expectations it entails. While it is difficult to imagine that an online market transaction is entered into without positive expectations at all, it is quite possible that many expectations are implicit and hard to enforce. Borderline cases would be, for example, market gambling (a deal is made although it is unlikely to hold) or automated ordering and selling (a deal is made by software agents based on routine calculations).

Vulnerability is common in online market settings and we should distinguish at least two different qualities of vulnerability in this context. First, an online deal may fail when a party does not fulfill its contractual obligations and the others lose something as a result, i.e. a payment already made, a product or service already delivered, time wasted, or an alternative deal forgone. Second, parties are vulnerable to a possible abuse of in-

formation that was shared in order to perform the transaction, but can be used for other purposes, too. Fraud and libel denote the more dramatic forms of abuse, but spam and gossip can be harmful nuisances just the same. The first type of vulnerability (e.g. a failed deal) is far more calculable than the second type (e.g. abuse of credit card details), hence the former may be seen as a matter of risk, while the latter involves uncertainty in the Knightian sense where stakes and probabilities are unknown (see Knight, [1921]1971) and where trust goes beyond calculation. The precondition of uncertainty is also fulfilled in online marketplaces more generally, because the actors involved have imperfect knowledge and control. In particular, trust becomes relevant especially when unforeseen technical problems occur, which the actors handle responsibly or carelessly, proving or disproving their trustworthiness.

Finally, we can assume that the users and providers of online market places have a choice in whether they participate and that they exercise agency also in the way they treat their transaction partners and accept responsibility. Those who do not have positive expectations will most likely choose not to become active in online market settings, as long as there are still offline alternatives. At the same time, transactions in online marketplaces are embedded in larger institutional frameworks of both formal and informal rules ranging from specific rules for a given marketplace to more general rules of online trading to the national laws created offline but applicable to online activities, too, such as legal provisions on retail, banking, tax, anti-trust, consumer protection, and privacy. Given the internet's global reach and the sometimes vague identity of actors involved, it is often hard to assess which institutions are applicable and even harder to enforce rights and duties. This makes trust both more difficult and more important. Nevertheless, market activities on the internet are embedded in social structures that shape expectations and behaviors.

Relevance of Trust in Online Communities and Social Networking

While the e-commerce activities referred to above have existed for much longer and have evolved more gradually into more interactive formats, social networking sites are most typical for the new possibilities of "Web 2.0", because it is through MySpace, Facebook, LinkedIn, Friendfeed, Twitter, and the like that users shift and manage a significant part of their social lives onto the web where they upload, update, link up, and communicate personal information within more or less extensive networks. Social networking sites usually give their users various options, for example, in labeling information as private or public so that users have control, apparently, over what information can be accessed by whom (boyd/Ellison, 2007). This is where trust becomes relevant, though. First, the provider who stores the data knows everything and may alter or ignore the restrictions set by the user. Second, other users who are classified as friends and have access to more sensitive information may equally violate the restrictions and publish the information elsewhere. Third, relatively harmless public data stored on different sites may become quite powerful and potentially damaging when they are combined using search engines or applications such as Yasnii. Hence, we observe how users struggle to manage their own online identities and reputations using technology such as OpenID or provider platforms such as ClaimID and myON-ID while other users and providers develop business models based on technologies that create links between traces and footprints that users leave online and exploit this information for dating, marketing, recruitment, or worse.

Considering the preconditions of trust's relevance more specifically, the main actors involved are the members of online communities (who use social networking sites), the providers (who run and maintain the sites), and third parties (who are

interested in the data stored on the site). Social relationships in which trust plays a role are established between users who link up actively through the site but who may also gather information about each other without a confirmed bilateral link. Users also have a relationship with the site providers who may be connected to various third parties that are thus linked indirectly to the sites' users, too. Like in online marketplaces, different types of actors have different relationships and different trust issues. The overall trusting expectation, though, is that correct information is provided, for the sites would be useless without, and that the data must not be abused, or else users will withdraw them or no longer provide any. A social networking site without such positive expectations is bound to be a dysfunctional collection of errors and lies, but not a place for trust.

Vulnerability and uncertainty are still very salient in online community settings, though, because even a minority of actors can harm individual users and the whole community while there is no certainty that no such users will gain access to sensitive data. Even if many of the activities on social networking sites are rather playful and trivial, one must not forget that real actors with offline lives are behind the online users, providers, and onlookers. The damage can be emotional or material, light or severe. The common use of pseudonyms, usernames, avatars and other fictional identities does not solve trust issues. The harm mostly still gets through to the person behind the fake identity who may be unable, however, to establish the real identity of the perpetrator. Hence, we believe that this practice offers only limited protection but raises the perception of vulnerability and uncertainty – and thus the need for trust. This is exacerbated by the fact that the possibility of covering one's tracks and erasing one's footprints is very limited online.

Still, millions of people are very active in online communities. Social networking sites continue to be seen as an attractive business opportunity for providers, too. Nobody is forced to participate,

but many choose to do so voluntarily and, more importantly, the main question is whether they do so responsibly. As long as there is also evidence of incompetent and malevolent agency, each user and provider faces a choice of being part of an online social network or not. Once again, this choice is not made in isolation but embedded in online and offline structures that influence the decision. For example, the choice may be limited to the range of existing sites, participation in one network may be more effective if one also uses other sites in parallel, and pre-existing offline communities may instigate their members to go online, too. Furthermore, online communities are governed by the same offline privacy regulations that apply to any association, organization, or individual, but that may be harder to control and enforce online.

Systemic Trust Problems Preventing Simplistic Solutions

In this section we support and extend the relevance of trust further by highlighting the systemic nature of trust issues in online settings. We have touched upon this point already, but it needs to be emphasized again, because much of the literature gives the impression that trust problems can be contained within particular applications, such as an online shop or social networking site, by implementing appropriate incentives and technologies to control access and information flows (Gefen et al., 2003; Wang & Emurian, 2005). In other words, the emphasis is on designing interfaces and applications in a 'trustworthy' fashion, but without paying much attention to the real actors and relationships that are (merely) mediated by technology and who have to accept any remaining vulnerability and uncertainty that cannot be eliminated by technology (nor, as Thiedeke [2007, p. 335 ff.] would argue, by distrust and power). Moreover, appealing and easy-to-use websites that elicit trust can be designed by honest and dishonest actors alike. This points to a signaling game that makes trust apparently impossible (Dasgupta, 1988) or a matter of

faith (Möllering, 2009). According to Bacharach and Gambetta (2001, p. 159), only those signals of trustworthiness are reliable that would be too costly for an inherently untrustworthy trustee to fake. In contrast to Dasgupta (1988) who argues that an inherently untrustworthy trustee has an even bigger incentive to send (fake) signals of trustworthiness than the inherently trustworthy trustee – which means that the signals are actually useless per se – Bacharach and Gambetta (2001) point out that it may take substantially more effort to mimic a signal than to send it naturally. However, signaling theory only moves the trust problem to another level and, in practice, trust in an online website cannot be guaranteed by careful design but remains an individual accomplishment of the users (see Möllering, 2006, pp. 41 ff.) who suspend the possibility that they may be deceived by a trustworthy-looking website or by the false and unverifiable claims of a platform provider (e.g. their policing of rogue users).

It should be noted again that, in times of “Web 2.0”, it is simply too narrow to study whether users find the website of an online shop trustworthy or whether they are willing to risk buying something or entering their postal address at a particular site. The vulnerability and uncertainty that make trust relevant come increasingly from the dense interconnections between sites rather than from individual sites. Users cannot even draw on simple search engines or news pages anymore without entering a system that is designed to find out who they are and what they like, with the aim of tailoring advertising and content to their presumed interests and preferences (see various contributions in Zimmer & Spink [2008]).

The literature on reputation systems for online applications looks overly simplistic to us, too, because such systems, or rather provider platforms, give the impression that trustworthiness is calculable (e.g. 99 percent positive evaluations) and they mainly shift the problem to the reliability of the reputation system (e.g. that scores are not inflated or distorted in any way). At best, such systems

are designed to increase control (see, for example the studies by Bolton et al., 2004, 2008; Bolton & Ockenfels, 2006), but they cannot eliminate vulnerability and uncertainty completely, which means that they leave the core of the trust problem unsolved. Furthermore, reputation systems also increase the interconnectedness of different online settings, especially when evaluations are invited, obtained, and posted by intermediaries such as price comparison services. The prospect that users will evaluate each other more and more on the internet, for everybody else to see, is not a very favorable one in our opinion, because these practices will create additional vulnerability and uncertainty for all involved, as past evaluations may forever haunt the poster just like the object.

Overall, we hope to have shown that trust is a general problem that is relevant in any online setting but that does not have a general solution to it, especially not one that addresses only the design of online media. We need to identify the actual social relationships that are (merely) technologically mediated, to establish the expectations, vulnerability, and uncertainty that they hold, and to take in both the agency of the individual actors as well as their embeddedness in social systems. The online world is a particular challenge for trust, because of the size and complexity of social networks that it enables and because of the broad but shallow embeddedness it draws on. In the next section, we address how trust can be socially constituted under these circumstances.

THE SOCIAL CONSTITUTION OF ONLINE TRUST

A General Framework for Explaining Trust

If trust is relevant in online settings, then we can draw on extensive literature aimed at explaining how trust comes about. In the following, we will use Möllering’s (2006) integrative framework,

which is derived from a critical review of existing trust theory. It distinguishes three perspectives on trust and highlights the leap of faith (*suspension*) as the key element required in all forms of trust.

In the first and most common perspective, trust is as matter of reason in the sense of a rational choice on the part of a trustor about his/her relationship with a given trustee. Accordingly, trust is based on a calculation of interest and utility, informed by the trustor's perception of the trustee's trustworthiness. There is much research on perceived trustworthiness and the types of criteria that trustors use, for example ability, benevolence, and integrity (Mayer et al., 1995). In the end, the trustor grants or withholds trust according to the expected value of the decision, like making a bet. This view suggests that trust can be increased through specific incentives, alignment of interests, and reliable signals of trustworthiness.

In the second perspective distinguished by Möllering (2006), trust is a matter of routine. In many social interactions in everyday life, it is taken for granted that people will give and honor trust – without calculating expected values every time. This trust is based on legitimate role expectations and appropriate role performances, and the recognition of what one should normally do. In other words, trust is not only protected by institutionalized rules, but institutionalized itself, that is, it is a usually unquestioned rule. Trust becomes stronger in this view, the less people think about it and the more they perform the trusting pattern automatically. Distrust, however, may equally become a hard-to-change routine.

In the third perspective that is very common in the literature, trust is a matter of reflexivity, meaning that it is based on experience and learning and has to be built more or less gradually. It is not a closed and static calculation, nor a mere repetition, but a combination of experimentation and reflection from one trust situation to the next. The trustor is able to engage with others even when calculations and routines are still impossible. Ac-

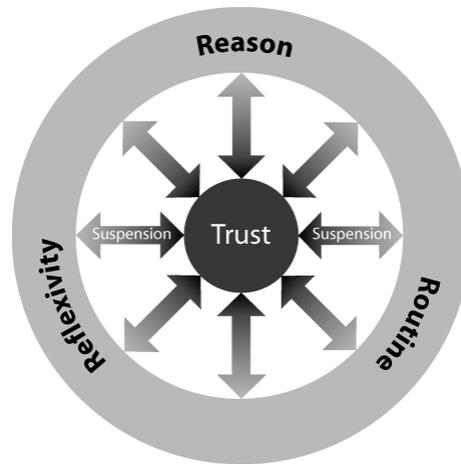
cordingly, trust is constituted when actors gain positive experiences in new situations.

We will discuss shortly how reason, routine, and reflexivity shape trust in online settings, but we need to emphasize that, in the framework we propose, trust is not to be confounded with its bases. In order to speak of trust as positive expectations in the face of vulnerability and uncertainty – beyond a rational choice, routine behavior, or past experience – there has to be a kind of leap of faith, i.e. the suspension of remaining doubt, uncertainty, and ignorance (Möllering, 2001). It is the special characteristic of trust that people interact *as if* things will go well, although they cannot be sure. This is a special emotional accomplishment and we will see what this means for users of online media.

In addition to the bases for trust and the leap of faith it involves, it is important to consider how the positive expectations of trust are experienced and enacted by the trustor. It is an empirical question, whether trust is experienced primarily as a positive emotion and intrinsic value, or whether trust is more of a burden and a source of anxiety even when positive expectations are in place. This is because in some settings actors would prefer to be able to interact without having to trust and in other settings it is the trust which makes the interaction particularly worthwhile. Similarly, when trust is present, it can be enacted in very different ways, even through inaction, or it may not be enacted at all.

The analysis of trust using the general framework outlined here needs to consider the part of the trustee, too. After all, the trustor responds to signals sent by the trustee regarding his/her interests and utility, trustworthiness, role acceptance, openness, and attitude towards vulnerability and uncertainty. Research and practice have an interest in understanding better the implications of the various, complex signaling games taking place online (see above; Bacharach & Gambetta, 2001). They give trustors and trustees many opportunities, and at least as many threats, to send

Figure 1. The trust wheel (Möllering 2006, p. 110)



and receive trust-relevant signals responsibly, playfully, deceptively, and so on. While ‘virtual’ entities are accepted and welcome as part of the online world, fakes and liars are not. The question is how to facilitate leaps of faith – ultimately an ‘illusion’ of certainty – without misleading the trustor irresponsibly. Interestingly, deception may be both invited and avoided through trust (see Möllering [2009] for a more extensive discussion).

We will demonstrate in the following sections that our framework is useful for gaining a better, more differentiated understanding of the constitution of trust in online marketplaces versus social networking media. The framework is based on the “Trust Wheel” (Figure 1, see Möllering 2006, p. 110) which shows that trust is based on reason, routine, and reflexivity, enabled by suspension. The positive expectation of trust is manifested in the experience and enactment on the part of the trustor.

Trust Constitution in Online Marketplaces

Online marketplaces would appear to be a paradigmatic setting for trust as a rational choice, based on calculating utility and assessing the trustworthiness of transaction partners. The

calculative approach matches the relatively low complexity of the interactions, where vulnerability and uncertainty are supposedly limited to distinct transactions, i.e. relatively clear potential gains and losses, mostly standardized information requirements, short-term involvement with the exchange partner, and easy exit. Yet, all of these assumptions are problematic and the constitution of trust between strangers in markets is actually not as easily explained by reason as it seems.

To start with, as research on the moral hazard problem of online trading and auctioning platforms such as eBay demonstrates (e.g. Bolton et al., 2004, 2008; Bolton & Ockenfels, 2006), markets work better if the actors involved do not consider merely the immanent transaction but also their respective reputations which they gained in prior deals and which they need for future activities in the market. Hence the online market should become a market for reputation, as it were, in that a peer-to-peer control system is installed whereby transaction partners rate each other and prices are qualified by the perceived trustworthiness of the actors involved. Bolton, Ockenfels and their colleagues believe that trust problems in online markets can be solved rationally by setting the right incentives within the trading platform, especially the incentive to maintain a

positive reputation based on past performance. Matzat (2009) shows that besides “direct control tools” such as these rating systems there are also the more contextual and relational “frame stabilizing tools” and “indirect monitoring tools”. However, reliance on all these tools presumes that reputations and past behaviors can be known objectively, that the underlying online systems are safe, and that trading decisions can be made rationally. This kind of research tends to overlook that trust is not only an issue between buyers and sellers, but also between both these groups and the platform providers. The latter have an interest in inflated reputations, because this will increase trading activity. They also prefer not to incur high costs of monitoring and sanctioning the market participants. In sum, when designing markets with the aim of alleviating their inherent trust dilemmas, the rational trust problem is transferred partly to the market designers and providers.

If there are limits to explaining trust in online marketplaces as a matter of rational choice, then we need to look at routines, because online traders may be following certain scripts and play their prescribed roles without calculating utility and reputation in every transaction (Berger & Luckmann, 1966). Through isomorphism (DiMaggio & Powell, 1983), i.e. doing as everybody else does, it is likely that more and more actors become users of online marketplaces, because it is seen as ‘normal’ to buy certain things online on well-known websites, especially books, music, or holidays. From the perspective of trust research what is interesting in this regard is that trust is based on taken-for-grantedness and familiarity. Calculativeness re-enters only when things do not unfold as expected. The providers of online market places make use of this route to trust by designing interfaces in such a way that they look familiar to users (e.g. shopping carts and baskets) and by communicating impressive numbers of users, suggesting that ‘everybody’ is using this website and that it is completely normal to register and participate. Users themselves engage in a kind

of Garfinkelian normalization process when they blame failed transactions on the dishonesty of a particular transaction partner or perhaps even on their own incompetence rather than questioning the platform and its provider more fundamentally (see Garfinkel, 1967). This would be evidence of a highly routinized and institutionalized trust in an online marketplace, e.g. if everybody is using Amazon and eBay and nobody can imagine that they could be set up in any other way than they currently are.

The reflexivity perspective of trust is also relevant to online market places, besides reason and routine, because users may well find themselves in unfamiliar situations where they can neither calculate expected utility nor follow a routine script. Instead it is through learning by doing that they develop trust (or distrust) in other users and in a given platform and its provider. Thus, trading partners do not need to trust each other to the full extent at the outset of a trust relationship. They can engage in a form of as-if trust which can gradually produce genuine trust, or fail to develop further (Möllering, 2006, pp. 77-104; see also Beckert, 2005). For the trustful functioning of an online marketplace, it is important that trust is not only dyadic but develops throughout a network of users in their relationships with each other and with the platform provider. However, reflexivity-based trust takes time and effort – and it is not ‘safe’ either, because it may involve many disappointments and set-backs along the way. The leaps of faith required to get a positive spiral of trust started are particularly demanding, even when one follows what Luhmann (1979) called the principle of gradualness, i.e. starting with small steps into a new trust relationship. Engaging in online market places always requires the suspension of vulnerability and uncertainty (Möllering, 2006, pp. 105 ff.), because neither calculations, nor routines, nor experiential learning can be perfect. Users may always doubt what they see on the screen. If they choose to ‘proceed to check-out’ with positive expectations nevertheless, this is an enactment

of their trust. In some instances, the behavior of online buyers and sellers may be better described as risk-taking, gambling, desperation, or foolishness. But we can speak of trust if an actor has positive expectations in spite of some remaining dangers.

As users of online platforms gain experience with this medium over time, their experiencing of trust in practice needs to be studied, too. It is telling in itself that some auction platforms advertise the excitement of participating in a bid, making even relatively trivial sales a matter of high emotional involvement. This extends to the question of whether the transaction partner will actually perform the deal after the auction is closed or the item has been ordered. At the same time, when users experience an auction positively or negatively in terms of trust, this always shapes their perception not only of their transaction partners but the platform providers, too. This is why it should be in the interest of platform providers to eliminate untrustworthy users, even if these users generate a lot of traffic, because their bad reputation may spill over to the whole platform. In order to enhance the users' positive experience, platform providers use techniques such as congratulating the transaction partners on their deal, thus making them feel good about their trust. Finally, to generate business, trust in online market places needs to translate into action. A platform cannot be sustained, if its users find each other trustworthy, but hardly anybody is really buying or selling anything. And the kind of trust that is involved in electronic markets is expressed most effectively by actual market activity. Leaps of faith are completed by mouse clicks, so to speak.

Trust Constitution in Online Communities and Social Networking

Reason, routine and reflexivity are categories that can be used to understand how trust is built in different settings. Comparing the online marketplaces considered above with online communities and social networking sites, the element of reason

and rational choice changes its meaning, because the utility of participating in online communities and social networks is often an end in itself. One participates not just to acquire items or pieces of information for offline use but in order to become part of a community. A good reputation and an extensive network of contacts here is not just a means to finding transaction partners but a measure of one's status and standing in the community. What this means is far less calculable in practice than the prices and percentage of satisfied customers in marketplaces. Online communities are designed to encourage their members to have as many contacts as possible, but beyond this maxim of "the more, the better", the exact motivations, payoffs and possible losses in online relationships are unclear. And it is a shallow basis for trust to believe that other users will not abuse their network contacts simply because they are afraid to lose some of these contacts as a result. As users join online communities and play with the different ways of managing their own identity and place in a network, the utility and trustworthiness of others are not calculated in advance but the product of participation. Nevertheless, social networking sites can be compared and distinguished meaningfully by the degree to which their members base their trust on estimated individual payoffs from participation (e.g. finding out about a job vacancy) versus taking participation to be the main payoff in itself (e.g. enjoying the chats with online friends). The utility for the provider of a networking platform might be just to enable a particular community of which the provider is a member, but it is often also a commercial interest of receiving participation fees, selling online advertising space, or collecting marketing profiles – which is much more interesting and problematic from a data protection and trust perspective. In order not to lose users, providers must signal the competent and benevolent treatment of personal information. In the end, though, users remain vulnerable to abuses by providers as well as other users.

Rational choice considerations are clearly relevant for trust in social networking, but also limited in explanatory power. Hence it should be fruitful to adopt the next perspective in our framework, i.e. trust as a matter of routines and taken-for-grantedness. To start with, while many older internet users may be reluctant to post their profiles on a website, younger users may already find this a completely normal thing to do in their daily lives. If, as far as they can see, everybody (in their offline world) is doing this and non-participation in Facebook, MySpace and so on is seen as the exception, then users will approach the online social media with relatively high trust in the websites and their users. It is important that this is not necessarily a naïve or even foolish type of trust, because the institutionalized rules and roles in established online communities and social networks may very well be highly reliable. Both the adherence to rituals such as a Twitter greeting in the morning or the inclusion of emoticons in text on the one hand and the reliable condemnation of unacceptable behavior among users on the other hand signal the normal working of an online community. What makes routine trust different from utility-based trust is that trustors do not have to calculate every time whether they should trust, but can adopt this as the default attitude and behavior – which is something that the providers of social media strongly promote, just like the providers of online marketplaces want users to think that it is completely normal to buy online. Even strongly institutionalized routines can still be broken, though, by untrustworthy users as well as providers. For example, when a provider changes the rules – as Facebook attempted in February 2009 – it may severely disrupt the routine expectations and undermine the trust in its services.

However, especially given the new formats for social networking and not to mention the new providers of such platforms that appear all the time, routines are not always in place yet and neither are reliable bases for rational decision making before entering a new community. This is where the re-

flexivity perspective of trust applies. Users – and also providers as trustees – learn gradually about the trustworthiness of a website and the other users who seek to form a community over it or at least to find a forum for their own interests. Reflexivity as a basis for developing trust is also analytically important, as was already mentioned in relation to marketplaces, because users may be using multiple websites and their good or bad experiences with one online community will affect how they interact subsequently within other communities. According to the principle of gradualness (Luhmann 1979), people may leave only small and rather harmless pieces of information about themselves online, but then extend this and end up managing a complex personal identity online within their main communities. This is important when studying, for example, Facebook users. Among the hundreds of millions of users of this platform, many may be only experimenting a bit with a relatively low profile while others organize almost their entire social life around, within, and through this community. For providers, user recruitment may be facilitated if new users do not need to enter too much information initially when they first set up a profile. For users, the positive feedback from initial experiences with a community may lead them to enter ever more information about themselves and become somewhat imprudent, because the safety and trustworthiness of a community is overestimated based on extrapolations from the past that may not hold once really sensitive data are revealed. The reflexivity perspective makes us aware of the users' online and offline histories and reminds us that individual action is not just a matter of the general incentive structures and routines that can be drawn upon at a particular point in time in an online environment.

Participation in online communities always carries a degree of vulnerability and uncertainty that reason, routine and reflexivity cannot entirely eliminate. Even relatively innocent traces left online may be combined and abused by malevolent others, be it members of the same communities or

outsiders who hack their way into the communities' databases. Against this background, users who participate with positive expectations have made a leap of faith. They act and interact as if the remaining dangers were unproblematic. It is hard to imagine that this is not what happens in most of the well-established online communities. The alternative would be that the majority of their members participate in a state of fear, coercion or desperation, not really expecting trustworthy behavior from the others but merely hoping that nothing bad will happen or even resigning to the fact that they will be taken advantage of. We cannot rule this scenario out completely, but when studying trust in online communities the more interesting question is how the other users and also the providers of the platforms promote the suspension of fear and doubt.

Enabling the leap of faith is closely related to the experiencing and enacting of trust in online communities. First, as in offline communities, the positive experience of feeling protected and respected within a trusted community is quite important. It needs to be maintained by the members of the community and in social networks this happens through the countless little messages that users send to support and comfort each other or to intervene when unacceptable behaviors occur. Trust is enacted not only by uploading personal information, but also by displaying one's responsibility, solidarity, and commitment to the other members. When trust is no longer enacted, an online community will become dysfunctional and probably dissolve before long, its members migrating to other platforms or withdrawing from online associations. In order to avoid this, online communities should be open for newcomers but display a virtual "Friends only!" sign above their virtual points of entry (see Möllering 2009, p. 146) as well as making sure that those who do not behave like friends are expelled. Friendship, here, is a matter of self-selection. By entering, the visitor commits himself to the rules of friendly behavior, irrespective of whether he or she is ac-

tually also an offline acquaintance of the owner of a weblog or profile.

The above reflections illustrate how our framework for studying trust in online settings can be applied to both online marketplaces and online communities. The main ideal-typical difference between the two forms of interaction on the internet remains that marketplaces are mostly used for short-term exchanges and brief encounters while communities are mostly used to manage longer-term identities and lasting relationships. Yet, the economic sphere of marketplaces and communal association in communities are densely interconnected. They have in common that the providers of the platforms want their users to "keep coming back" and that utility, routines, and learning processes are involved in the constitution of trust among users and between users and providers.

TOWARD A METHODOLOGY FOR THE EMPIRICAL STUDY OF ONLINE TRUST

Based on the analytical framework we have outlined and the specific issues around the complexity and interrelatedness between online settings as noted earlier on in the chapter, this section presents basic implications for the design of future empirical research in this field. The empirical study of trust online remains unsatisfactory, as long as trust online is conceptualized only as trust in a technology or incentive structure, because users do not only encounter specific websites but build their online biographies navigating across many parts of the internet. Their vulnerability lies much less in losing small things here and there than in losing control over their scattered online lives that are not disconnected from their offline realities. While online artifacts of all sorts represent important data, it is crucial to understand the various real and potential connections between all the traces, profiles, conditions of usage, and so on. To achieve this, we think that researchers

need to meet with users in person to learn in depth about their intentions, decisions, and experiences related to the problem of trust. This is required to understand better the actual practices of using online marketplaces or social networks. We suggest a praxeological approach to trust, focusing on actors, their social relations, and their practices of integrating the internet into their daily lives. We think that trust in online settings is better explained on the basis of dense online biographies than on the basis of large datasets about isolated online interactions.

A variety of methods offer promising approaches for the empirical study of trust online. The methods that we advocate briefly below are all making use of online technology to a greater or lesser extent. This is an advantage when studying people who use such technologies already anyway. More conventional techniques are more appropriate perhaps for non-users or those who have been upset by bad experiences on the internet. Each method can be used individually in smaller projects but a combination of these methods should be particularly fruitful in larger research projects on trust in online settings:

1. **Online surveys:** Respondents can be self-recruiting or be invited to the survey via email or regular mail. This method is problematic if it is not very open and interactive. Its potential can be increased if respondents are given the opportunity to offer detailed reflections and upload digital material that illustrates their online activities (Welker et al., 2005). It would also be desirable to create longitudinal panel data instead of just cross-sectional samples in order to get closer to the idea of analyzing online biographies. Qualitative interviews with at least a subsample of the survey respondents should also be considered.
2. **Laboratory experiments:** The main objective in using this method would be to observe users in real time as they are using online

marketplaces and communities. Ideally, this should be with real websites that the users would go to outside of the lab situation, too, but more classical laboratory experiments with simulated websites and different treatments could be instructive, too, as long as the main interest is not in optimal web-design but in understanding how actors draw on their online histories when encountering a new site.

3. **Case studies:** This method aims for a dense description of an online marketplace or social networking platform and its offline context (see, for example, Geertz, 1977). Crucially, the research team needs to look behind the scenes. It is not enough to analyze the software and data involved in running the platform, i.e. the traces that are left naturally. Building on ethnographic techniques it is necessary to gain insights into the motivations and decisions of the platform providers and users, which will mostly not be documented already on the platform itself.
4. **Expert interviews:** This type of interviewing is not a data gathering exercise by an expert researcher but a conversation of the researcher with experts in the field who offer their insights and explanations on the phenomenon under study. For trust in online settings, the experts to be considered can be anyone with extensive experience, which includes users and providers as well as slightly more detached journalists, activists, IT specialists, or academics. The internet may be used to conduct the interviews (e.g. Skype). As an alternative to interviewing, the experts can also be asked to keep a diary on their online activities and reflections with regard to trust.
5. **Online forums:** Presuming that many trust issues in online settings are already discussed spontaneously by users in various chat rooms and blogs, it may be fruitful to create

a platform dedicated to this topic where all parties concerned can voice their concerns and report their experiences. Such an online forum (e.g. weblog) could be established as part of a website of a larger research project on online trust and be moderated by the researchers. The aim of this method would be to identify relevant issues and topical cases coming directly from the users' lives world, without claiming representativeness.

6. **Barcamps:** In the spirit of developing research methods that draw on new forms of interaction that have emerged from the online world, it would be particularly interesting to set up a self-organizing conference, known as a barcamp, on the topic of trust in online settings. The barcamp itself is an offline activity where anybody who is interested in the topic can meet with others face-to-face. The preparation of the barcamp is largely done online, though, and it is an important feature of this format that participants are posting their presentations, comments, twittering et cetera online, thereby creating qualitative data that can be used fruitfully in a trust research project.

These methodological suggestions build on conventional methods but encourage researchers, first, to make use of internet technology and online artifacts as well as, second, to try and get as close as possible to the practices and interpretations of users. In particular, the leap of faith that characterizes trust is an idiosyncratic, highly emotional accomplishment by trustors and this requires researchers to get close to the moment of experiencing and enacting trust (see also Barbarlet, 2009; Möllering, 2001)

CONCLUSION

In the offline world, trust is required in specific interactions and, more generally, as a basis for

getting involved in the first place. Everybody using the internet is confronted with the choice to trust or to keep out, that is, limit the degree and scope of internet usage as long as they are distrusting. Everybody who chooses to participate, though, remains vulnerable, even if they have positive trusting expectations. The uncertainty about whether one will be harmed can only be suspended, not eliminated, because it is impossible to identify all sources of potential failure, transform them into risks, assign probabilities and mathematically manage risk in order to avoid failure (see Power, 2007, pp. 66-102). A wary, reluctant, and distrustful attitude paralyzes users but contributes no additional security to the internet. Trust, in contrast, helps to overcome paralysis by combining good reasons with the benefit of the doubt and a cooperative, but not foolish, stance.

In our opinion, the sheer size, growth, and global interconnectivity of the internet rule out an effective centralized regulation of all online marketplaces, communities and the internet as a social sphere. Control or political governance as a more abstract form of control, if seen as an alternative to trust, is not a viable alternative in this field, contrary to the conclusions of, for example, Thiedeke (2007). Trust, in contrast, can be built up in decentralized processes and then lead to more generalized rules, roles, and routines that become institutionalized and taken for granted by all users across a range of online marketplaces and communities. In this chapter, we have proposed a broad framework that captures the elements involved in the constitution of trust. We underline that trust is not primarily an abstract property of a social system but a very personal and practical experience, stretching out in time and space, both online and offline. Hence it is not enough, in research or practice, to be concerned with the trust-effective design of individual websites or devices, as has been common to date. Trust is a social process spanning online biographies of users and the life course of provider platforms. Trusting actors are aware that trust concerns arise as a consequence of

their participation, but they are prepared to make a leap of faith. Since users, providers, developers, and the general public alike are related to each other as trustors and trustees simultaneously, each party must offer a favorable self-definition and cooperate to produce a desirable internet of trust.

REFERENCES

- Bacharach, M., & Gambetta, D. (2001). Trust in signs. In Cook, K. S. (Ed.), *Trust in Society* (pp. 148–184). New York: Russell Sage Foundation.
- Baier, A. (1986). Trust and antitrust. *Ethics*, 69(2), 231–260. doi:10.1086/292745
- Barbalet, J. (2009). A characterization of trust, and its consequences. *Theory and Society*, 38(4), 367–382. doi:10.1007/s11186-009-9087-3
- Beckert, J. (2005). Trust and the Performative Construction of Markets. *MPIfG Discussion Paper* 05/8. Cologne, Germany: Max Planck Institute for the Study of Societies.
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3/4), 245–270. doi:10.1016/S0963-8687(02)00018-5
- Benkler, Y. (2006). *The wealth of Networks. How Social Production transforms Markets and Freedom*. New Haven, CT: Yale University Press.
- Berger, P. L., & Luckmann, T. (1966). *The Social Construction of Reality*. Garden City, NY: Doubleday.
- Bolton, G., Loebecke, C., & Ockenfels, A. (2008). Does competition promote trust and trustworthiness in online trading? An experimental study. *Journal of Management Information Systems*, 25(2), 145–169. doi:10.2753/MIS0742-1222250207
- Bolton, G. E., Katok, E., & Ockenfels, A. (2004). Trust among internet traders. A behavioral economics approach. *Analyse & Kritik*, 26, 185–202.
- Bolton, G. E., & Ockenfels, A. (2006). *The Limits of Trust in Economic Transactions. Investigations of Perfect Reputation Systems*. Retrieved from http://ockenfels.uni-koeln.de/uploads/tx_ockmedia/Bolton_Ockenfels_Limits_of_Trust.pdf
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1). Retrieved from <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.
- Brinkmann, U., & Seifert, M. (2001). Face to Interface: Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen. *Zeitschrift für Soziologie*, 30(1), 23–47.
- Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 28(6), 737–758. doi:10.1016/S1071-5819(03)00041-7
- Das, T. K., & Teng, B.-S. (1998). Resource and Risk Management in the Strategic Alliance Making Process. *Journal of Management*, 24(1), 21–42. doi:10.1016/S0149-2063(99)80052-X
- Dasgupta, P. (1988). Trust as a commodity. In Gambetta, D. (Ed.), *Trust: Making and Breaking Co-operative Relations* (pp. 49–72). Oxford, UK: Basil Blackwell.
- Diaz, A. (2008). Through the Google Goggles: Sociopolitical bias in Search Engine Design. In Zimmer, M., & Spink, A. (Eds.), *Web Search. Multidisciplinary Perspectives* (pp. 11–34). Heidelberg, Germany: Springer.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. doi:10.2307/2095101

A Framework for Studying the Problem of Trust in Online Settings

- Eimeren, B., & Frees, B. (2008). *Internettuwauchs: Größter Zuwachs bei den Silversurfern. Ergebnisse der ARD/ZDF-Onlinestudie 2008*. Retrieved from http://www.daserste.de/service/studie08_1.pdf
- Garfinkel, H. (1967). *Studies in Ethnomethodology*. Englewood Cliffs, NJ: Prentice Hall.
- Geertz, C. (1977). *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *Management Information Systems (MIS) Quarterly*, 27(1), 51–90.
- Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783–812. doi:10.1016/S1071-5819(03)00043-0
- Guenther, T., & Schmidt, J. (2008). Wissenstypen im Web 2.0 – eine wissenssoziologische Deutung von Prodnutzung im Internet. In Willems (Ed.). *Weltweite Welten. Figurationen aus wissenssoziologischer Perspektive* (pp. 167-187). Wiesbaden, Germany: VS-Verlag.
- Habermas, J. (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: Polity Press. (Original work published 1962)
- Hess, A. (2008). Reconsidering the Rhizome. A textual analysis of Web Search engines as Gatekeepers of the Internet. In Zimmer, M., & Spink, A. (Eds.), *Web Search. Multidisciplinary Perspectives* (pp. 35–50). Heidelberg, Germany: Springer.
- Knight, F. H. (1971). *Risk, Uncertainty, and Profit*. Chicago: University of Chicago Press, Phoenix Books. (Original work published 1921)
- Lessig, L. (2004). *Free Culture. The nature and future of creativity*. New York: Penguin.
- Long, C. P., & Sitkin, S. B. (2006). Trust in balance: How managers integrate trust-building and task control. In Bachmann, R., & Zaheer, A. (Eds.), *Handbook of Trust Research* (pp. 87–106). Cheltenham, UK: Elgar.
- Lorenz, E. H. (1988). Neither friends nor strangers: Informal networks of subcontracting in French industry. In Gambetta, D. (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 194–210). New York: Blackwell.
- Luhmann, N. (1979). *Trust and Power: Two Works by Niklas Luhmann*. Chichester, UK: Wiley.
- Matzat, U. (2009). The Acceptance and Effectiveness of Social Control on the Internet: A Comparison between Online Auctions and Knowledge Sharing Groups. In Cook, K., Snijders, C., & Buskens, V. (Eds.), *Trust and Reputation*. New York: Russell Sage Foundation.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. doi:10.2307/258792
- McKnight, D. H., & Chervany, N. L. (2002). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), 35–59.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems*, 11(3/4), 297–323. doi:10.1016/S0963-8687(02)00020-3
- Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology*, 35(2), 403–420.
- Möllering, G. (2005). The trust/control duality: An integrative perspective on positive expectations of others. *International Sociology*, 20(3), 283–305. doi:10.1177/0268580905055478

- Möllering, G. (2006). *Trust: Reason, Routine, Reflexivity*. Amsterdam: Elsevier.
- Möllering, G. (2009). Leaps and lapses of faith: Exploring the relationship between trust and deception. In Harrington, B. (Ed.), *Deception: From Ancient Empires to Internet Dating* (pp. 137–153). Stanford, CA: Stanford University Press.
- PEW Internet & American Life Project. (2007a). *Online identity management and search in the age of transparency*. Retrieved from http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf
- PEW Internet & American Life Project. (2008a). *Online Shopping. Internet users like the convenience but worry about the security of their financial information*. Retrieved from http://www.pewinternet.org/pdfs/PIP_Online%20Shopping.pdf
- Power, M. (2007). *Organized Uncertainty. Designing a World of Risk Management*. Oxford, UK: Oxford University Press.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393–404.
- Shankar, V., Smith, A. K., & Rangaswamy, A. (2003). Customer satisfaction and loyalty in online and offline environments. *International Journal of Research in Marketing*, 20(2), 153–175.
- Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems*, 11(3/4), 325–344. doi:10.1016/S0963-8687(02)00022-7
- Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology*, 93(3), 623–658. doi:10.1086/228791
- Stewart, K. J. (2003). Trust transfer on the World Wide Web. *Organization Science*, 14(1), 5–17. doi:10.1287/orsc.14.1.5.12810
- Thiedecke, U. (2007). *Trust, but test! Das Vertrauen in virtuellen Gemeinschaften*. Konstanz, Germany: UVK.
- Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), 105–125. doi:10.1016/j.chb.2003.11.008
- Welker, M., Werner, A., & Scholz, J. (2005). *Online-Research. Markt- und Sozialforschung mit dem Internet*. Heidelberg, Germany: dpunkt.verlag.
- Zimmer, M. (2008). The Gaze of the Perfect Search Engine: Google as an Infrastructure of Dataveillance. In Zimmer, M., & Spink, A. (Eds.), *Web Search. Multidisciplinary Perspectives* (pp. 77–99). Heidelberg: Springer.