Development of Trust Measure in Biometric Technology

Zhaleh Semnani-Azad
Clarkson University
Reh School of Business
zsemnani@clarkson.edu

Shih-Yi Chien
National Chengchi University
Department of Information Management
sychien@nccu.edu.tw

Yannick Forster
Chemnitz University of Technology
Yannick.Forster@s2017.tu-chemnitz.de

Stephanie Schuckers
Clarkson University
Department of Electrical and Computer Engineering
sschucke@clarkson.edu

Houchao Gan
Clarkson University
Department of Electrical and Computer Engineering
ganh@clarkson.edu

Abstract

Societal acceptance of biometric technology is complex and highly dependent on trust. The limited work on trust in biometric s is mostly anecdotal with correlational patterns associated with familiarity and confidence in different types of biometric s [26]. *To develop a comprehensive understanding of people's trust perceptions toward biometric s, we employed existing theories to develop a systematic measure of trust in biometric s from a consumer perspective. We 1) gathered prior trust measures in the context of interpersonal interaction, technology adoption, information system and automated technology, 2) identified common trust dimensions across these contexts, 3) modified the items for the context of biometric technology, and 4) conducted a survey study to determine sub-factors and reliability of this new measure. Our data generated seven new factors associated with consumer trust in biometric technology. We discuss implications of the current work and suggest future directions.*

1. Introduction

Biometric technology is a type of technology that measures, accumulates data and potentially analyzes a person's physiological or behavioral characteristics [33]. These characteristics which are unique to each individual can be used to verify or identify that person. Biometric technology is preferred over traditional identification paradigms such as protected passwords, as a more reliable and accurate identification and verification technique [34]. While biometric technology is considered a more rigorous system for collecting and analyzing human data, it is prone to biases and provokes anxiety and discomfort among the people in which it measures [10]. For instance, privacy concerns influence user comfort level in biometric technology such as border security screening [12]. Privacy counsel for Europe indicates that privacy is one of the key factors of trust in information technology [31]. Accordingly, user trust and acceptance toward biometric technology is an important avenue to explore.

Trust is critical in determining people's behavior. Prior research found that privacy and trust are closely related in predicting people's willingness to disclose personal information [31]. Privacy concern is one of the major issues with Biometric technology; this factor may influence people's behavioral intention to use and or provide personal and physiological data to this type of technology. Interpersonal trust, or people's disposition to trust other individuals has a significant influence on how people trust technology in general [12]. For instance, people's trust level associated with individual differences and cultural norms predict the extent to which people trust automation [26]. Accordingly, we incorporate and extend on interpersonal trust to develop a fundamental understanding of trust in biometric s technology, and how trust mediates acceptance of biometric s technology. It is important to understand human factors associated with trusting biometric technology. Yet, to our knowledge there are no systematic trust measures of biometric technology.

The dearth of work that examined trust in biometrics were anecdotal, based on general correlational measures of people's acceptance toward this technology [26:5]. We employ existing theories and measures on (a) interpersonal trust, (b) trust in technology and (c) trust in automation, to develop a more refined measure of trust in biometric s. From prior research, we refine items associated with four starting dimensions of trust and implement these in the context of biometric al technology. These dimensions include: 1) *Ability* measures what functionality does biometric technology provide to users; 2) *Attitude* measures what users think about biometric technology; 3) *Behavior*

URI: https://hdl.handle.net/10125/60015
ISBN: 978-0-9981331-2-6

measures how users employ biometric technology; 4) *Ease of Use* measures how easy it is to use biometric technology. We test our modified measures with human subjects and examine the reliability of these dimensions in the context of biometric technology. We also propose new dimensions applicable to this type of technology. We then test the extent to which our refined measure predicts people's perception of trust in biometric technology in general, and how individual differences further influence trust levels.

The paper is organized as follows. First, after the prior literature review, we describe how four starting dimensions of trust were selected. Second, we detail the measure items and samples. Third, we explain how the three dimensions were extracted in the context of trusting biometric technology. Finally, we present the analysis of our data, discuss current results and future directions.

2. Prior Work

Prior empirical work has proposed the privacy-trust-behavioral intention model in e-commerce [21] in which people are more likely to trust and provide personal information if the privacy policy of an e-commerce website is fully disclosed. Biometric technology to some extent functions similar to an e-commerce business. Biometric s gathers people's personal information and physiological data for identification purposes. However, there are limitations in terms of the availability of accumulated data, people's access to that data, agents who have access to the data and the function of the gathered data. Accordingly, people are more likely to have low trust toward biometric s because of such privacy concerns [8, 27]. Thus, it is important for researchers to understand the factors that contribute to people's trust in biometric technology.

To our knowledge there are no trust measures developed in the biometric s context. However, prior literature does provide reliable trust measures in other domains. Interpersonal trust or people's disposition to trust others, heavily influences people's trust in general technology, automation, and information technology. Consequently, researchers have been successful at developing trust measures in these domains [10, 18, 19, 24]. While these domains are not in the context of biometric s, there are some similarities across these types of technologies, particularly in the realm of information accumulation and exchange [8, 27]. Thus we build on trust measures in these domains and adopt them in the context of biometric technology.

2.1 Interpersonal Trust Dimensions

Trust is a multidimensional construct [11]. Interpersonal trust reflects a person's willingness to be vulnerable to the actions of others based on positive expectations [26]. Thus far, majority of trust literature in terms of theoretical and empirical work fixate on interpersonal trust [6, 9, 13]. Interpersonal trust is important in biometric technology since this type of trust is highly predictive of people's trust in technology as a whole [6]. Rotter [30] proposed that interpersonal trust in a dyadic relationship arises from attributes associated with a trustee and a trustor in three types of situations: group, organization and individual. Within the group context, Jarvenpaa et al. [17] identified 6 dimensions of trust: Behavior, trustworthiness, ability, integrity, benevolence and propensity. In the organization context, Paine [28] proposed the following dimensions for interpersonal trust: Integrity, dependability, competence, honesty and vulnerability. For individual-level of interpersonal trust, prior studies [18–20] identified these dimensions: dependency, faith, belief, disposition and predictability. Table 1 provides a summary of these dimensions.

Table 1. Interpersonal trust dimensions from prior literature

Reference	Context	Trust Dimension	Theoretical Trust Dimension
[17]	Interpersonal trust in group	Behavior, Trustworthiness, Ability, Integrity, Benevolence Propensity	Behavior, Trustworthiness, Ability, Integrity, Benevolence, Reliability, Faith
[28]	Interpersonal trust in organization	Integrity, Dependability, Competence, Honesty, Vulnerability.	
[12, 29, 35]	Individual Interpersonal trust	Dependency, Faith, Belief, Disposition, Predictability.	

While these contexts give rise to many dimensions, i.e. sub-factors, capturing interpersonal trust, there are some overlaps among these factors with relevance to biometric technology. For instance, Paine [28] measured *honesty* as how much and how accurately information is shared between people in an organization. In a biometric s context, we can examine this from a uni-directional rather than a bi-directional perspective since there is only one linkage of people sharing information with the biometric technology and not the other way around. Similarly, Jarvenpaa et al. measured *propensity* as how personal traits influence the trustor's trust toward the trustee. In the context of

biometric s, we can examine the influence of personal traits and individual differences in trust level. Accordingly, we employ these prior dimensions from interpersonal trust framework as the theoretical basis for our trust measure.

2.2 Trust Dimensions in General Technology

Literature shows several empirical measures of trust in the context of general technology. These measures reflect the extent to which people adopt and use technology as a whole. Table 2 provides a summary of the dimensions/factors derived from trust in general technology measures.

Table 2. General technology trust dimensions from prior literature

Reference	Context	Trust Dimension	Theoretical Trust Dimensions
[1]	Trust in mobile banking technology	Perceived usefulness, Perceived ease of use, Credibility, the Amount of information, Normative pressure	Ability, Ease of Use, Reliability, Compatibility, Usefulness, Risk, Behavior, Functionality, Helpfulness, Attitude, Intension, Faith
[2]	Trust in mobile banking technology	Compatibility, usefulness, and Risk	
[4]	Trust in general technology	Attitude, Perceived ease of use, Perceived usefulness, Behavioral control, Subjective norm, Intention to adopt technology.	
[24]	Trust in general technology	Reliability, Functionality, Helpfulness, Faith	

Amin et al. [1] found that perceived usefulness, ease of use, credibility, the amount of information and normative pressure are meaningful factors predicting people's acceptance of technology, in the context of mobile banking. in a similar context, Koenig-Lewis et al. [2] identified compatibility, usefulness, and risk are significant factors for adoption of technology. Aboelmaged. [4] incorporated these factors to develop a behavioral measure capturing people's intent to use technology. In this work, trust dimensions of attitude, ease of use, usefulness, behavioral control, subjective norm and intention to adopt technology, were predictive of intentions. In another line of work, McKnigh et al. [24] developed a measure of trust in technology stemming from interpersonal trust measures. These researchers identified the following factors: reliability, functionality, helpfulness, and faith in general technology. In our work we implement the theoretical and conceptual framework of these factors into the domain of biometric technology. We use the dimensions listed in table 2 as the theoretical basis for trust in general technology.

2.3 Trust Dimensions in Information Technology (IT)

Consistent with the literature on trust in general technology, trust measures on information technology demonstrate factors and dimensions with a similar conceptual nature, also derived from interpersonal trust [24]. Faith in information technology, an index of trust, is a prevalent conceptual framework examined, which captures people's beliefs about various attributes of information technology. In this case, more faith in information technology reflects people's beliefs that information reliable, functional, and provides the necessary help needed. Extending on this work, Jarvenpaa et al. [18] proposed that user's trust in information technology (e.g. internet store) is dependent on reputation. Since trust involves risk [23], Jarvenpaa et al. also suggested that people's risk perceptions are highly indicative of trust in information technology. Thus, these dimensions expanded earlier factors identified in interpersonal trust and trust in general technology.

Similar to trust dimensions in tables 1-2, Riquelme and colleagues [14] found that ease of use, usefulness, norms, and social risk are factors that influence the intention to adopt information technology (e.g. online banking service). Extending these factors, Bhattacherjee [3] found that attitude, subjective norm and behavioral control can explain 52% of variance in predicting people's intention to use information technology (e.g. e-brokerage services). Thus, we also incorporate these theoretical models and items associated with these measures into the context of biometric technology. Since both biometric technology and information technology often require sharing information, we predict that these unique dimensions are valid for biometric s (see table 3).

Table 3. Information technology trust dimensions from prior literature

Reference	Context	Trust Dimension	Theoretical Trust Dimensions

[25]	Trust in general technology	Faith	Faith, Ease of Use, Reputation, Risk, Attitude, Usefulness, Subjective norm, Behavior
[18]	Trust in internet store	Risk Perception, Reputation	
[14]	Trust in online banking service	Ease of use, Usefulness, Social norms, Social risk	
[3]	Trust in general information technology	Attitude, Subjective norm, Behavioral control	

2.4 Trust Dimensions in Automation

Recent research in the automation technology developed a trust measure in this context with the incorporation of cultural factors [7], based on prior trust dimensions in automation [19]. The work expanded on factors mentioned earlier such as attitude, usefulness, ease of use, subjective norm, reliability, faith and behavioral intention associated with interpersonal trust [36], general technology [16] and information technology [32]. In addition to these factors, Hoff et al. [15] identified workload and complexity as unique dimensions for trust in automation. Biros et al. [5] confirmed that under high workloads, operators use automation more often to maintain pace with task demands, regardless of their level of trust. In another research, Lyons et al. suggested that under high-risk conditions, operators may have a tendency to reduce their reliance on complex automation, but increase their reliance on simple automation [22].

Since majority of trust dimensions in automation were derived from a system perspective, we propose that trust in biometric technology will also encompass these factors. Majority of work on trust in automation examine trust from the user's perceptive. Given that current biometric technology is incorporated into the general technology used by consumers, e.g. touch and fingerprint detection in smart phones, we also develop our trust in biometric s measure from the user or consumer perspective. Table 5 illustrates the summary of factors discussed in trusting automation and the theoretical conceptualization we plan to employ in our work.

Table 4. Automation trust dimensions from prior literature

Reference	Context	Trust Dimension	Theoretical Trust Dimensions
[7]	Trust in Automation	Attitude, Usefulness, Ease of Use, Subjective norm, Reliability, Faith and Behavioral Intention	Attitude, Usefulness, Ease of Use, Subjective norm, Reliability, Faith, Behavioral Intention, Workload, Complexity

2.5 Trust Dimensions in Biometric Technology

From these existing trust dimensions, we selected four dimensions that were in common across the contexts of interpersonal trust, trust in general technology, information technology and automation. Table 5 lists these dimensions. The conceptual definition of these factors are as follows: (1) *Ability* refers to the functionality of biometric technology; (2) *Attitude* refers to a user's judgment toward biometric technology based on prior experience and existing knowledge,; (3) *Behavior* refers to the user's belief toward future behavior, i.e. impact, of biometric technology based on prior experience and existing knowledge; (4) *Ease of Use* refers to the user's perceived effort in learning and using biometric technology. In our study we combined the items associated with these dimensions from the factors mentioned earlier. We modified these items to reflect consumer perspective on trusting biometric technology. We carried out an online study with general working population from Mechanical Turk to determine the reliability of these dimensions and the generation of new factors specifically associated with biometric technology.

Table 5. Trust dimensions with unique dimensions and shared dimensions

	Interpersonal	General Technology	Automation	Information Technology
Dimensions	Behavior, Trustworthiness, Ability, Integrity, Benevolence, Reliability, Faith	Ability, Ease of Use, Reliability, Compatibility, Usefulness, Risk, Behavior, Functionality, Helpfulness, Attitude, Intension, Faith	Attitude, Usefulness, Ease of Use, Subjective norm, Reliability, Faith, Behavioral Intention, Workload, Complexity	Faith, Ease of Use, Reputation, Risk, Attitude, Usefulness, Subjective norm, Behavior
Unique Dimensions	Integrity, Trustworthiness, Benevolence	Helpfulness, Reliability	Workload, Complexity	Reputation
Shared Dimension	**Behavior, Ability**	**Ease of use, Attitude, Ability, Behavior**	**Attitude, Ease of use**	**Ability, Behavior, Ease of use**

3. Current Research and Methods

3.1 Initial Scale Construction

Previous research [20] suggested a "dimension sampling" method, which assumes a predefined dimension of content for each measurable construct and select candidate items that can faithfully represent this domain. Accordingly, a three-step procedure was used to create items for the proposed trust scale and establish its content validity. 1) Relevant facets of each of the four starting trust dimensions were identified by conceptualizing them in the biometric technology context. 2) Items from prior trust literature reflecting each starting trust dimension were identified and modified to minimize semantic overlap across items. 3) Prior scale items that matched best with the starting trust dimensions were selected and reworded to relate specifically to the biometric technology context. New items were created to represent trust level from users' perspective. Most items were reworded in general biometric technology (e.g. I look forward to see more daily use biometric technology) to ensure that the proposed trust items are not specific to a particular type biometric technology, thus minimizing any extant biases in the trust dimensions (such as, personal preference). The number of items for the proposed trust dimensions was 25. This number ensures that survey takers can finish all items in 10-15 minutes in order to obtain a desired reliability. Further, it is important to keep our measurement scales as short as possible to minimize respondent fatigue.

The first phase of scale construction required specifying items for each of our four trust dimensions: Ability, Attitude, Behavior and Ease of Use. Ability refers to user's perception that biometric technology has the necessary functionalities, and meets most of the user's needs. Attitude refers to user's judgment of biometric technology based on pre-existing knowledge and concerns of private user information and previous experience. Behavior identified as whether or not the technology makes users intent or continue to use based on their current experience. Ease of Use is identified as whether or not the technology demonstrates helpfulness and usefulness toward user concerns and needs, and makes good-faith efforts to resolve user concerns.

In the second phase, pervious research trust measure items were reviewed again. From prior trust measurements, items that met 3 conditions were selected. Items were selected based on whether they, (1) examined one of the four starting dimensions of trust, (2) could be adapted to assessing user's trust in biometric technology, and (3) did not overlap with any of the study's other constructs. Items with substantial semantic overlap were merged into a single item. For instance, the items "Technology is changing too fast for me." [28] and "It is too difficult to keep up with advancements in technology." [3] were grouped into one single "Ease of Use" item. Each item was reworded to relate specifically to biometric technology context (with user as the trustor) and anchored using a 5-point Likert scale ranging from "strongly disagree" to "strongly agree."

The final phase was to reduce the initial item pool to 25 items representing each of the four dimensions of trust. Item reduction and refinement were conducted by (1) directly changing the context to biometric technology or (2) completely rewriting the items.

3.2 Task and Procedure

Participants for this study were Amazon Mechanical Turk workers. The participants were 100 random selected workers from U.S and 100 random selected workers from India. A survey link instruction was generated. The introduction outlined the purpose of the study, provided a hyperlink to an online survey form, and as an incentive, offered participants $0.4 after they completed survey. Participants were 31% female with a mean age of 34.0 years. All participants were given a brief introduction about biometric technology before completing the survey items. Participants were asked to rate their opinion about each statement associated with the consumer perspective of biometric technology (see Table 8).

4. Analysis and Result

Reliability analysis was performed on responses for each four starting dimensions. Skewness for all measure items average responses ranged between -0.9 and -0.56, kurtosis ranged between 0.8 and 1.51, within the -2 to +2 range, which identified reasonably normal distributional properties for the Mechanical Turk data.

The initial trust measures were modeled as a four-factor model, with 7 items measuring ability, 7 items measuring attitude, 5 items measuring behavior, 5 items measuring ease of use and 1 general trust measure in biometric technology. The reliability analysis is shown in Table 6. These response are considered reliable (Cronbach's alpha is higher than 0.7).

Principal component analysis (PCA) combined with Varimax and Kaiser Normalization rotation method was employed to extract new features (in this case, we tried to extract new dimensions/factors). Three new factors were extracted with eigenvalue greater than 1, since 1 is considered as an average eigenvalue, therefore grater 1 is considered as above average. The new three factor model (Table 7) explains 59.1% of the variance associated with trust in biometrics.

Table 6. Reliability statistics for starting dimensions

Starting Dimensions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Num of Items
Ability	0.822	0.830	7
Attitude	0.873	0.876	7
Behavior	0.872	0.874	5
Ease of Use	0.787	0.789	5

Table 7. Reliability statistics for extracted dimensions

Extracted Dimensions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Num of Items
Factor 1	0.953	0.954	19
Factor 2	0.884	0.887	7
Factor 3	0.815	0.817	6

Next, rotated component matrix was performed to examine the factor loading for each item (Table 8). Results of the rotated component matrix will be used to refine our items for future empirical research. Based on the factor loading and new group items, we marked Factor 1 as "Functionality", Factor 2 as "Intention" and Factor 3 as "Ease of Use" (Table 8). Functionality is defined as users' trust toward biometric technology, based on whether the technology has met most of the user's needs. In this case, security and privacy can be considered as one of important sub dimensions in functionality from empirical data. For instance, items "Biometric technology keeps users information safe during most time.", "I would be able to use biometric technology well for securing personal information" and "I find that biometric technology useful in managing personal information." with high loading factor for Factor 1 suggest that privacy and security have great impact when users think about a biometric technology. Intention is defined as user's willingness to transform and employ biometric technology. For instance, "I read about advancements in biometric technology." illustrates user trust and willingness to use biometric technology by gathering more information about biometric technology. Ease of use is defined as the difficulty level for users to use biometric technology. Unlike other type of technology, ease of use can be defined as the usefulness and helpfulness of biometrics. In this case, users were more concerned about the difficulty level of biometric technology and the difficulty level of gathering information about biometric technology.

Table 8. Mechanical Turk data collection FA (factor analysis) results: The values represented the factor loadings for each item. The model of specific items with a threshold value 0.4, in order to eliminate the noise.

Rotated Component Matrix[a]

	Component		
	1	2	3
I generally trust biometric technology	.725		
I would use camera face detection function to take picture.	.585		
I would use iris scan function to access my expensive laptop.	.433	.624	
I would use fingerprint scan function to access my bank account.	.554		
I would use a voice control system to drive a car.		.710	
I would use a voice recognition typing system to writing an essay.			.604
Biometric technology has the ability of meet most user needs.	.626		.424
Biometric can provide excellent service.	.681		
Biometric technology makes daily life more convenient.	.687		
I like using the biometric technology.	.694	.422	
I look forward to see more daily use biometric technology.	.647		
Biometric technology keeps users information safe during most time.	.777		
Biometric technology make personal information more private.	.641		
Using the biometric technology is NOT frustrating for me.			.667
I intend to use the latest biometric technology in the next year.	.538	.589	
I plan to use the newest biometric technology (e.g. Google's Trust API) in the next 12 months.	.616	.544	
I would be able to use biometric technology well for securing personal information	.709		
Using biometric technology is entirely within my control.	.567		
I find that biometric technology useful in managing personal information.	.779		
I get excited when I use a new biometric technology.	.420	.666	
I read about advancements in biometric technology.		.720	
Overall, I believe that biometric technology is easy to use.	.467		.542
I would NOT feel apprehensive about using the biometric technology.			.571
It is NOT too difficult to keep up with advancements in biometric technology.			.776
Biometric technology is compatible with other technology I use.	.595		

5. Discussion and Future Directions

The purpose of this paper was to develop and validate an instrument for measuring users' trust in biometric technology. Scale construction is one of the most important steps in confirmatory research because the quality of a measurement items determines the extent to which observed results are meaningful and accurate. As discussed before, prior trust scales were not directly applicable to biometric technology. Based on four starting dimensions of trust adopted from prior trust measurements (ability, attitude, behavior and ease of use) in biometric technology contexts, an initial three factor model was constructed (Table 8).

The development of a trust scale in this paper is part of a larger study examining the impact of cultural factor in trusting biometric technology. In future studies we will examine how cultural norms associated with general societal trust impacts trusting biometric technology. We expect the results of this research to provide a reliable psychometric instrument that captures the nature and antecedents of trust in biometric s across cultures. The current measures focus on biometric technology in general, and trust from a consumer's perspective. For future work, we plan on investigating whether trust varies with different types of biometric technology. We will also examine people's trust perceptions when they are required to use biometric

technology, e.g. crossing border, identification technology at work, etc… Finally, one of the interesting and value-added areas is machine learning, where we can classify high trust of biometric technology users and low trust biometric technology users based on our proposed dimensions (features). We expect a linear separation between high versus low trust in biometric technology users.

6. Acknowledgment

This material is based upon work supported by the Center for Identification Technology Research and the National Science Foundation under Grant No. #1650503.

7. References

[1] Amin, H., Hamid, M.R.A., Lada, S., and Anis, Z. The Adoption of Mobile Banking in Malaysia: The Case of Bank Islam Malaysia Berhad (bimb). *International Journal of Business and Society; Sarawak 9*, 2 (2008), 43-53,76-77.

[2] Anita Lifen Zhao, Nicole KoenigLewis, Stuart HanmerLloyd, and Philippa Ward. Adoption of internet banking services in China: is it all about trust? *International Journal of Bank Marketing 28*, 1 (2010), 7–26.

[3] Bhattacherjee, A. Acceptance of e-commerce services: the case of electronic brokerages. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 30*, 4 (2000), 411–420.

[4] Bhattacherjee, A. Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems 19*, 1 (2002), 211–241.

[5] Biros, D.P., Daly, M., and Gunsch, G. The Influence of Task Load and Automation Trust on Deception Detection. *Group Decision and Negotiation 13*, 2 (2004), 173–189.

[6] Boudreau, M.-C., Gefen, D., and Straub, D.W. Validation in Information Systems Research: A State-of-the-Art Assessment. *MIS Quarterly 25*, 1 (2001), 1–16.

[7] Chien, S.-Y., Lewis, M., Hergeth, S., Semnani-Azad, Z., and Sycara, K. Cross-Country Validation of a Cultural Scale in Measuring Trust in Automation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting 59*, 1 (2015), 686–690.

[8] Cohn, M. Biometrics: Key to securing consumer trust. *Biometric Technology Today 15*, 3 (2007), 8–9.

[9] Compeau, D.R. and Higgins, C.A. Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly 19*, 2 (1995), 189–211.

[10] Darley, J. Review of Trust in Organizations: Frontiers of Theory and Research. *Business Ethics Quarterly 8*, 2 (1998), 319–335.

[11] Frewer, L.J., Howard, C., Hedderley, D., and Shepherd, R. What Determines Trust in Information About Food-Related Risks? Underlying Psychological Constructs. *Risk Analysis 16*, 4 (1996), 473–486.

[12] Gefen, D. E-commerce: the role of familiarity and trust. *Omega 28*, 6 (2000), 725–737.

[13] Hart, K.M., Randall, H., Cangemi, J.P., and Caillouet, L.M. Exploring organizational trust and its multiple dimensions: A case study of General Motors. *Organization Development Journal 4*, 2 (1986), 31–39.

[14] Hernan E. Riquelme and Rosa E. Rios. The moderating effect of gender in the adoption of mobile banking. *International Journal of Bank Marketing 28*, 5 (2010), 328–341.

[15] Hoff, K.A. and Bashir, M. Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors 57*, 3 (2015), 407–434.

[16] Hultberg, P.T., Nadiri, M.I., Sickles, R.C., and Hultberg, P.T. An International Comparison of Technology Adoption and Efficiency: A Dynamic Panel Model. *Annales d'Économie et de Statistique*, 55/56 (1999), 449–474.

[17] Jarvenpaa, S.L., Knoll, K., and Leidner, D.E. Is Anybody out There? Antecedents of Trust in Global Virtual Teams. *Journal of Management Information Systems 14*, 4 (1998), 29–64.

[18] Jarvenpaa, S.L., Tractinsky, N., and Saarinen, L. Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication 5*, 2 (1999), 0–0.

[19] Jiun-Yin Jian, Bisantz, A.M., and Drury, C.G. Foundations for an Empirically Determined Scale of Trust in Automated System. *International Journal of Cognitive Ergonomics 4*, 1 (2000), 53.

[20] Jum C, N. *Psychometric theory*. Auflage, New York ua: Mc Graw-Hill, 1978.

[21] Liu, C., Marchewka, J.T., Lu, J., and Yu, C.-S. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management 42*, 2 (2005), 289–304.

[22] Lyons, J.B. and Stokes, C.K. Human–Human Reliance in the Context of Automation. *Human Factors 54*, 1 (2012), 112–121.

[23] Mayer, R.C., Davis, J.H., and Schoorman, F.D. An Integrative Model of Organizational Trust. *The Academy of Management Review 20*, 3 (1995), 709–734.

[24] Mcknight, D.H., Carter, M., Thatcher, J.B., and Clay, P.F. Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Trans. Manage. Inf. Syst. 2*, 2 (2011), 12:1–12:25.

[25] McKnight, D.H. and Chervany, N.L. Trust and Distrust Definitions: One Bite at a Time. In *Trust in Cyber-societies*. Springer, Berlin, Heidelberg, 2001, 27–54.

[26] Nelson, L.S. *America Identified: Biometric Technology and Society*. MIT Press, 2010.

[27] P. G. W, K. Are you ready for the trust' economy? 1997.

[28] Paine, K.D. Guidelines-for-Measuring-Trust-KDP-4-13.pdf. 2003. http://www.instituteforpr.org/wp-content/uploads/Guidelines-for-Measuring-Trust-KDP-4-13.pdf.

[29] Rempel, J.K., Holmes, J.G., and Zanna, M.P. Trust in close relationships. *Journal of Personality and Social Psychology: Interpersonal Relations and Group Processes 49*, 1 (1985), 95–112.

[30] Rotter, J.B. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist 35*, 1 (1980), 1–7.

[31] Schofield, C. and Joinson, A. Privacy, Trust, and Disclosure Online. 2008. http://gsb.haifa.ac.il/~sheizaf/cyberpsych/02-PaineSchofield%26Joinson.pdf.

[32] Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly 27*, 3 (2003), 425–478.

[33] Wayman, J., Jain, A., Maltoni, D., and Maio, D. An Introduction to Biometric Authentication Systems. In J. Wayman, A. Jain, D. Maltoni and D. Maio, eds., *Biometric Systems*. Springer London, 2005, 1–20.

[34] Woodward, J.D., Webb, K.W., Newton, E.M., Bradley, M.A., and Rubenson, D. *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*. Rand Corporation, 2001.

[35] Yamagishi, T. The provision of a sanctioning system as a public good. *Journal of Personality and Social Psychology 51*, 1 (1986), 110–116.

[36] The Role of Espoused National Cultural Values in Technology Acceptance on JSTOR. http://www.jstor.org/stable/25148745.