

Chapter 3

Trusting Technological Actors: A Foundation in Structure and Cultural Sentiments

Daniel B. Shank
University of Georgia, USA

ABSTRACT

This chapter sets forth a theoretical foundation for studying trust toward technological actors as social actors using sociological research in structure and cultural sentiments. The introduction considers how modern intelligent technologies make human-technology trust a relevant and timely topic, while the background section reviews humans' social interaction with technology. Using social structure and cultural sentiments the author constructs four propositions about trusting technological actors. Two empirical research studies illustrate the cultural sentiment propositions showing trust in technological actors and violation of trust in computers. Throughout the chapter the author connects the sociological literature with everyday examples before providing grounded propositions that would be appropriate foundations for research in multiple disciplines.

INTRODUCTION

The source of any information affects people's trust in that information. We all have the experience of somebody believing something just because it came from a computer, sometimes according it higher trust for this reason, while others have the opposite response (Picard, 1997, p. 114)

It is not uncommon for people to trust global positioning systems to direct them to their destination, internet searches to bring up reliable information, stock prediction programs to make decent suggestions, and meteorology websites to predict upcoming weather. As developments are made in technology, there are several concurrent processes that are relevant to the importance of studying trust in technological actors. First, the capacity of technology allows it to be applied to new domains that previously were occupied only by humans. Domains where humans must trust in technologies to make

DOI: 10.4018/978-1-61520-901-9.ch003

decisions or predictions are vast including stock market and financial predictions, gaming, medical diagnostics, military and police intelligence, identity verification, online bidding systems, mobile network security systems, vehicle design configurations, vehicle stress simulations, and meteorology. Second, the complexity of the domains means that technologies are using stochastic and heuristic processes instead of deterministic processes. Artificial intelligence techniques used for designing systems in the aforementioned domains include pattern matching, simulated annealing, genetic and evolutionary algorithms, expert systems, rule-based learning with logic databases, distributed computing, simulations of environments and artificial neural networks. One domain and one technique I will use as an ongoing example is applying artificial neural networks to meteorological predictions. Artificial neural networks have been used in prediction of tornadoes, storms, solar radiation, carbon dioxide levels, pollutants, ozone concentration, sulfur dioxide concentration, and precipitation (Gardner & Dorling, 1998), tide charts (Steidley, Sadowski, Tissot, & Bachnak, 2005), ocean waves levels (Wedge, Ingram, McLean, Mingham, & Bandar, 2005), flash floods (Luk, Ball, & Sharma, 2000), fog (Nugroho, Kuroyanagi, & Iwata, 2002), air temperature (Jain, McClendon, Hoogenboom, & Ramyaa, 2003; Smith, McClendon, & Hoogenboom, 2006), and dew point temperature (Shank, Hoogenboom, & McClendon, 2008; Shank, McClendon, Paz, & Hoogenboom, 2008). Like artificial neural networks and weather prediction, a huge number of software applications, computational systems, and domains have important, nondeterministic technologies making trust in technological actors a timely topic.

In this chapter I begin by arguing that humans treat technologies socially, and therefore people's trust or distrust in them can be informed by sociological theory. Next, I review a limited sociological literature on trust, focusing on social structure and cultural sentiments as antecedents of

trust. As I review the literature, I apply theoretical principles from network theories and Affect Control Theory to technological actors in the form of propositions. Last, I conclude by reviewing two current Affect Control Theory research projects on cultural sentiments, trust, and technological actor interaction.

BACKGROUND

There are many different approaches to studying trust in technological actors. A number of studies investigate technologies' influence on organizations (DiMaggio, Hargittai, Neuman, & Robinson, 2001; Liker, Haddad, & Karlin, 1999; Podolny & Stuart, 1995; Shortliffe, 1993; Stuart & Podolny, 1996) and even how technological actors function as members of organizations (Carley, 2002). Actor-Network Theory (Callon & Latour, 1992; Latour, 2005) suggests that technology has been socially constructed to be a separate domain from the human-social realm, and to address this construction theorists analyze technology and humanity from the same standpoint. This moves technological actors, not humans, to the center of socio-cultural life and narratives (Latour, 1996). Likewise, science and technology studies look at science, technology, and knowledge as cultural products that are constructed (Bijker, 1995; Collins, 1995) and how they affect other systems such as culture, governments, communications (Jasanoff, Markle, Peterson, & Pinch, 1995), and privacy (Karat, Karat, & Brodie, 2008). All of these approaches contribute to the perspective adopted in this chapter, but are not fully reviewed within.

In Human-Computer Interaction (HCI) research one perspective called Computers Are Social Actors (CASA) is used as background for the propositions developed in this chapter. CASA is a research tradition based in psychological social-psychology and communications that proposes that people treat computers and other technologies socially. "Socially" means

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/trusting-technological-actors/42899

Related Content

Challenges in Sharing Computer and Network Logs

Adam Slagelland Kiran Lakkaraju (2010). *Collaborative Computer Security and Trust Management* (pp. 64-80).

www.irma-international.org/chapter/challenges-sharing-computer-network-logs/39381

Analyzing the Ethical Dilemma between Protecting Consumer Privacy and Marketing Customer Data

Utpal Bose (2011). *International Journal of Dependable and Trustworthy Information Systems* (pp. 55-68).

www.irma-international.org/article/analyzing-ethical-dilemma-between-protecting/78292

Security and Trust of Public Key Cryptography for HIP and HIP Multicast

Amir K.C, Harri Forsgren, Kaj Grahm, Timo Karviand Göran Pulkkis (2011). *International Journal of Dependable and Trustworthy Information Systems* (pp. 17-35).

www.irma-international.org/article/security-trust-public-key-cryptography/78290

STRIDE: A Secure Framework for Modeling Trust-Privacy Tradeoffs in Distributed Computing Environments

Rima Deghaili, Ali Chehab, Ayman Kayssiand Wassim Itani (2010). *International Journal of Dependable and Trustworthy Information Systems* (pp. 60-81).

www.irma-international.org/article/stride-secure-framework-modeling-trust/43582

The Role of Trust in Online Relationship Formation

Andrew T. Fioreand Coye Cheshire (2010). *Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives* (pp. 55-70).

www.irma-international.org/chapter/role-trust-online-relationship-formation/42900