# Tragedy, truth, and technology: the 3t theory of social media-driven misinformation

N Roberts, H Qahri-Saremi

Year:2023

<https://aisel.aisnet.org/jais/vol24/iss5/3/>

## Abstract

Abstract  
False claims and misinformation on social media have substantially increased in the last few years. Some people have incorrectly interpreted such content as the truth, sometimes to the extent that it transforms their view of reality and subsequently leads to actions that cause harm and suffering. Despite the burgeoning body of research on misinformation on social media, we know little about the process by which social media-driven misinformation shapes and reinforces false beliefs that result in detrimental outcomes. Building on insights from dramaturgical tragedy, theories of truth, and research on social media, we develop a process theory that explains how social media-driven misinformation transforms a person’s view of reality in a way that leads to detrimental human action.

# Mitigating information asymmetry to achieve crowdfunding success: signaling and online communication

N Wang, H Liang, Y Xue, S Ge

Year:2021

<https://aisel.aisnet.org/jais/vol22/iss3/4/>

## Abstract

Abstract  
This paper examines how signals and the herding factor originating from multiple sources complement or substitute for each other’s effects in the crowdfunding context. Drawing on the elaboration likelihood model, we propose that signals from campaigns (videos) and creators (experience) can mitigate information asymmetry concerns about project quality and creator credibility and that creator-originating signals offset the effect of campaign-originating signals on crowdfunding success. Further, we posit that online communication between creators and backers (backer comments and creator replies) complements or substitutes for the effects of signals originating from the campaign or creator. We collected and analyzed objective data on 9,884 crowdfunding projects from a major reward-based crowdfunding platform in China and were able to confirm most of our hypotheses.

# Texting with humanlike conversational agents: Designing for anthropomorphism

AM Seeger, J Pfeiffer, A Heinzl

Year:2021

<https://aisel.aisnet.org/jais/vol22/iss4/8/>

## Abstract

Abstract  
Conversational agents (CAs) are natural language user interfaces that emulate human-to-human communication. Because of this emulation, research on CAs is inseparably linked to questions about anthropomorphism—the attribution of human qualities, including consciousness, intentions, and emotions, to nonhuman agents. Past research has demonstrated that anthropomorphism affects human perception and behavior in human-computer interactions by, for example, increasing trust and connectedness or stimulating social response behaviors. Based on the psychological theory of anthropomorphism and related research on computer interface design, we develop a theoretical framework for designing anthropomorphic CAs. We identify three groups of factors that stimulate anthropomorphism: technology design-related factors, task-related factors, and individual factors. Our findings from an online experiment support the derived framework but also reveal novel yet counterintuitive insights. In particular, we demonstrate that not all combinations of anthropomorphic technology design cues increase perceived anthropomorphism. For example, we find that using only nonverbal cues harms anthropomorphism; however, this effect becomes positive when nonverbal cues are complemented with verbal or human identity cues. We also find that CAs’ disposition to complete computerlike versus humanlike tasks and individuals’ disposition to anthropomorphize greatly affect perceived anthropomorphism. This work advances our understanding of anthropomorphism and contextualizes the theory of anthropomorphism within the IS discipline. We advise on the directions that research and practice should take to find the sweet spot for anthropomorphic CA design.

# Have we crossed the uncanny valley? Understanding affinity, trustworthiness, and preference for realistic digital humans in immersive environments

M Seymour, LI Yuan, A Dennis…

Year:2021

<https://aisel.aisnet.org/jais/vol22/iss3/9/>

## Abstract

Abstract  
Developers have long strived to create virtual avatars that are more realistic because they are believed to be preferred over less realistic avatars. However, an “uncanny valley” exists in which avatars trigger aversion when they are almost but not quite realistic. We used a field study to investigate whether users had different affinity, trustworthiness, and preferences for avatars with two levels of realism, one that was close to human-realistic and one a cartoon caricature. We observed behavior, conducted one-on-one interviews, and collected survey data from SIGGRAPH conference attendees who either participated in a live discussion session between two avatars in a VR environment, or observed it via 3D VR headsets or on a large screen 2D video display. Eighteen sessions were conducted over four days, with the same person animating the human-realistic avatar and different guests animating the caricature avatars. The guests who interacted with the human-realistic avatar had a positive experience in the VR environment. The observers had positive evaluations of both avatars while acknowledging their different levels of realism. They rated the human-realistic avatar as more trustworthy, had more affinity for it, and preferred it as a virtual agent. Participants who observed the interview through VR headsets had an even stronger affinity for the human-realistic avatar and stronger preferences for it than those who observed via the 2D screen. Effect sizes ranged from medium to large. Our results suggest that it is now possible to cross the uncanny valley with human-realistic avatars rendered in real time.

# Thinking technology as human: affordances, technology features, and egocentric biases in technology anthropomorphism

JF Zheng, S Jarvenpaa

Year:2021

<https://aisel.aisnet.org/jais/vol22/iss5/3/>

## Abstract

Abstract  
Advanced information technologies (ITs) are increasingly assuming tasks that have previously required human capabilities, such as learning and judgment. What drives this technology anthropomorphism (TA), or the attribution of humanlike characteristics to IT? What is it about users, IT, and their interactions that influences the extent to which people think of technology as humanlike? While TA can have positive effects, such as increasing user trust in technology, what are the negative consequences of TA? To provide a framework for addressing these questions, we advance a theory of TA that integrates the general three-factor anthropomorphism theory in social and cognitive psychology with the needs-affordances-features perspective from the information systems (IS) literature. The theory we construct helps to explain and predict which technological features and affordances are likely: (1) to satisfy users’ psychological needs, and (2) to lead to TA. More importantly, we problematize some negative consequences of TA. Technology features and affordances contributing to TA can intensify users’ anchoring with their elicited agent knowledge and psychological needs and also can weaken the adjustment process in TA under cognitive load. The intensified anchoring and weakened adjustment processes increase egocentric biases that lead to negative consequences. Finally, we propose a research agenda for TA and egocentric biases.

# The perils and promises of big data research in information systems

V Grover, A Lindberg, I Benbasat…

Year:2020

<https://aisel.aisnet.org/jais/vol21/iss2/9/>

## Abstract

Abstract  
With the proliferation of “big data” and powerful analytical techniques, information systems (IS) researchers are increasingly engaged in what we label as big data research (BDR)—research based on large digital trace datasets and computationally intensive methods. The number of such research papers has been growing rapidly in the top IS journals during the last decade, with roughly 16% of papers in 2018 employing this approach. In this editorial, we propose five conjectures that articulate the potential consequences of increasing BDR prevalence for the IS field’s research goals and outputs. We discuss ways in which IS researchers may be able to better leverage big data and new analysis techniques to conduct more impactful research. Our intent with these conjectures and analyses is to stimulate debate in the IS community. Indeed, we need a productive discussion about how emerging new research methods, digital trace data, and the development of indigenous theory relate to and can support one another.

# Who is the next “wolf of wall street”? Detection of financial intermediary misconduct

J Lausen, B Clapham, M Siering…

Year:2020

<https://aisel.aisnet.org/jais/vol21/iss5/7/>

## Abstract

Abstract  
Financial intermediaries are essential for investors’ participation in financial markets. Because of their position within the financial system, intermediaries who commit misconduct not only harm investors but also undermine trust in the financial system, which ultimately has a significant negative impact on the economy as a whole. Building upon information manipulation theory and warranting theory and making use of self-disclosed data with different levels of external verification, we propose different classifiers to automatically detect financial intermediary misconduct. In particular, we focus on self-disclosed information by financial intermediaries on the business network LinkedIn. We match user profiles with regulator-disclosed information and use these data for classifier training and evaluation. We find that self-disclosed information provides valuable input for detecting financial intermediary misconduct. In terms of external verification, our classifiers achieve the best predictive performance when also taking regulator-confirmed information into account. These results are supported by an economic evaluation. Our findings are highly relevant for both investors and regulators seeking to identify financial intermediary misconduct and thus contribute to the societal challenge of building and ensuring trust in the financial system.

# Integrating cognition with an affective lens to better understand information security policy compliance

D Ormond, M Warkentin, RE Crossler

Year:2019

<https://aisel.aisnet.org/jais/vol20/iss12/4/>

## Abstract

Abstract  
Information systems security behavioral research has primarily focused on individual cognitive processes and their impact on information security policy noncompliance. However, affective processes (operationalized by affective absorption and affective flow) may also significantly contribute to misuse or information security policy noncompliance. Our research study evaluated the impact of affective absorption (i.e., the trait or disposition to allow one’s emotions to drive decision-making) and affective flow (i.e., a state of immersion with one’s emotions) on cognitive processes in the context of attitude toward and compliance with information security policies. Our conceptual model was evaluated using a laboratory research design. We found that individuals who were frustrated by work-related tasks experienced negative affective flow and violated information security policies. Furthermore, perceptions of organizational injustice increased negative affective flow. Our findings underscore the need for understanding affective processes as well as cognitive processes which may lead to a more holistic understanding regarding information security policy compliance.

# The effects of media capabilities on the rationalization of online consumer fraud

A Harrison

Year:2018

<https://aisel.aisnet.org/jais/vol19/iss5/1/>

## Abstract

Abstract  
This research develops and tests a model of online consumer fraud to determine how the capabilities of communication technologies affect the rationalization of fraudulent behaviors. The model is based on research about the rationalization of fraud, media capabilities, and computer-mediated deception. This investigation empirically tests this model by analyzing 459 Facebook advertisements and 1,896 surveys completed by university students. The findings indicate that the capabilities provided by communication technologies affect the extent to which media mask cues of deceit and dehumanize others. As a result, some media capabilities increase one’s willingness to engage in fraudulent behaviors while other capabilities deter those actions. Media capabilities that mask cues of deceit and reduce social presence increase the inclination of individuals to rationalize fraudulent activities, while media capabilities that expose cues of deceit and increase social presence deter individuals from rationalizing acts of fraud. Media offering greater capabilities for reprocessability and transmission velocity decrease the inclination to rationalize fraud, whereas greater capabilities for anonymity, rehearsability, and parallelism increase the inclination to rationalize fraud. In contrast, symbol set variety does not appear to significantly affect the inclination to rationalize fraud.

# Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance

JB Barlow, M Warkentin, D Ormond…

Year:2018

<https://aisel.aisnet.org/jais/vol19/iss8/3/>

## Abstract

Abstract  
Organizations use security education, training, and awareness (SETA) programs to counter internal security threats and promote compliance with information security policies. Yet, employees often use neutralization techniques to rationalize noncompliant behavior. We investigated three theory-based communication approaches that can be incorporated into SETA programs to help increase compliance behavior: (1) informational communication designed to explain why policies are important; (2) normative communication designed to explain that other employees would not violate policies; and (3) antineutralization communication designed to inhibit rationalization. We conducted a repeated measures factorial design survey using a survey panel of full-time working adults provided by Qualtrics. Participants received a SETA communication with a combination of one to three persuasion statements (informational influence, normative influence statement, and/or an antineutralization), followed by a scenario description that asked for their intentions to comply with the security policy. We found that both informational (weakly) and antineutralization communication (strongly) decreased violation intentions, but that normative communication had no effect. In scenarios where neutralizations were explicitly suggested to participants, antineutralization communication was the only approach that worked. Our findings suggest that we need more research on SETA techniques that include antineutralization communication to understand how it influences behavior beyond informational and normative communication.

# Got phished? Internet security and human vulnerability

S Goel, K Williams, E Dincelli

Year:2017

<https://aisel.aisnet.org/jais/vol18/iss1/2/>

## Abstract

Abstract  
A leading cause of security breaches is a basic human vulnerability: our susceptibility to deception. Hackers exploit this vulnerability by sending phishing emails that induce users to click on malicious links that then download malware or trick the victim into revealing personal confidential information to the hacker. Past research has focused on human susceptibility to generic phishing emails or individually targeted spear-phishing emails. This study addresses how contextualization of phishing emails for targeted groups impacts their susceptibility to phishing. We manipulated the framing and content of email messages and tested the effects on users’ susceptibility to phishing. We constructed phishing emails to elicit either the fear of losing something valuable (e.g., course registrations, tuition assistance) or the anticipation of gaining something desirable (e.g., iPad, gift card, social networks). We designed the emails’ context to manipulate human psychological weaknesses such as greed, social needs, and so on. We sent fictitious (benign) emails to 7,225 undergraduate students and recorded their responses. Results revealed that contextualizing messages to appeal to recipients’ psychological weaknesses increased their susceptibility to phishing. The fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing. The results of our study provide important contributions to information security research, including a theoretical framework based on the heuristic-systematic processing model to study the susceptibility of users to deception. We demonstrate through our experiment that several situational factors do, in fact, alter the effectiveness of phishing attempts.

# Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)

A Vance, BB Anderson, CB Kirwan…

Year:2014

<https://aisel.aisnet.org/jais/vol15/iss10/2/?wptouch_preview_theme=enabled>

## Abstract

Abstract  
Users’ perceptions of risks have important implications for information security because individual users’ actions can compromise entire systems. Therefore, there is a critical need to understand how users perceive and respond to information security risks. Previous research on perceptions of information security risk has chiefly relied on self-reported measures. Although these studies are valuable, risk perceptions are often associated with feelings—such as fear or doubt—that are difficult to measure accurately using survey instruments. Additionally, it is unclear how these self-reported measures map to actual security behavior. This paper contributes to this topic by demonstrating that risk-taking behavior is effectively predicted using electroencephalography (EEG) via event-related potentials (ERPs). Using the Iowa Gambling Task, a widely used technique shown to be correlated with real-world risky behaviors, we show that the differences in neural responses to positive and negative feedback strongly predict users’ information security behavior in a separate laboratory-based computing task. In addition, we compare the predictive validity of EEG measures to that of self-reported measures of information security risk perceptions. Our experiments show that self-reported measures are ineffective in predicting security behaviors under a condition in which information security is not salient. However, we show that, when security concerns become salient, self-reported measures do predict security behavior. Interestingly, EEG measures significantly predict behavior in both salient and non-salient conditions, which indicates that EEG measures are a robust predictor of security behavior.

# Is this review believable? A study of factors affecting the credibility of online consumer reviews from an ELM perspective

CMY Cheung, CL Sia, KKY Kuan

Year:2012

<https://aisel.aisnet.org/jais/vol13/iss8/2/>

## Abstract

Abstract  
With the ever-increasing popularity of online consumer reviews, understanding what makes an online review believable has attracted increased attention from both academics and practitioners. Drawing on the elaboration likelihood model (ELM), this study examines four information cues used to evaluate the credibility of online reviews: Argument quality, source credibility, review consistency, and review sidedness, under different levels of involvement and expertise. We conducted an online survey that involved users of Epinions.com, a popular online consumer review website, to test the research model empirically. Consistent with previous research, the results reveal that argument quality, a central cue, was the primary factor affecting review credibility. Participants also relied on peripheral cues such as source credibility, review consistency, and review sidedness when evaluating online consumer reviews. Review sidedness had a stronger impact on review credibility when the recipient had a low involvement level and a high expertise level. However, the other interaction effects were not significant. We discuss the theoretical and practical implications of these results.

# The evolution of interaction networks in massively multiplayer online games

J Putzke, K Fischbach, D Schoder…

Year:2010

<https://aisel.aisnet.org/jais/vol11/iss2/2/>

## Abstract

Abstract  
This article examines the co-evolution of players’ individual performance and their interaction network in a Massively Multiplayer Online Game (MMOG). The objective is to test whether the application of theories from the real world is valid in virtual worlds. While the results indicate that the structural effects and demographic variables active in the real world influence the evolution of the players’ interaction network in MMOGs (e.g. transitivity, reciprocity, and homophily), they do not provide evidence that players’ structural embeddedness in the interaction network influences player performance. These findings have important implications for researchers and practitioners who need to understand social processes in MMOGs (e.g., when launching marketing campaigns in MMOGs) or who study MMOGs and then use their findings to draw conclusions about the real world (e.g., when analyzing the relationship between employee performance and network structure).

# A hybrid attribute selection approach for text classification

CH Chou, AP Sinha, H Zhao

Year:2010

<https://aisel.aisnet.org/jais/vol11/iss9/1/>

## Abstract

Abstract  
The application of text mining in organizations is growing. Text classification, an important type of text mining problem, is characterized by a large attribute space and entails an efficient and effective attribute selection procedure. There are two general attribute selection approaches: the filter approach and the wrapper approach. While the wrapper approach is potentially more effective in finding the best attribute subset, it is cost-prohibitive in most text classification applications. In this paper, we propose a hybrid attribute selection approach that is both efficient and effective for text classification problems. We apply the proposed approach to detect and prevent Internet abuse in the workplace, which is becoming a major problem in modern organizations. The empirical evaluations we conducted using a variety of classification algorithms, indexing schemes, and attribute selection methods demonstrate the utility of the proposed approach. We found that combining the filter and wrapper approaches not only boosts the accuracies of text classifiers but also brings down the computational costs significantly.

# Avatars, people, and virtual worlds: Foundations for research in metaverses

A Davis, J Murphy, D Owens, D Khazanchi…

Year:2009

<https://aisel.aisnet.org/jais/vol10/iss2/1/>

## Abstract

Abstract  
Metaverses are immersive three-dimensional virtual worlds in which people interact as avatars with each other and with software agents, using the metaphor of the real world but without its physical limitations. The ubiquitous availability of high speed Internet access has spurred enormous interest in virtual worlds like Second Life and World of Warcraft, both in terms of user gaming and as a new technological platform for global virtual collaboration. These environments have potential for richer, more engaging collaboration, but their capabilities have yet to be examined in depth. Of particular interest in this paper is the use of metaverses for virtual team collaboration. We develop a conceptual model for research in metaverses that is based on five key constructs: (1) the metaverse itself, (2) people/avatars, (3) metaverse technology capabilities, (4) behaviors, and (5) outcomes. We present an in-depth characterization of metaverse technology capabilities from a socio-technical view that recognizes the potential for variation in emergent interaction and in outcomes. Example propositions and a discussion of key issues and challenges show how the model can be used to further research and practice in virtual teams in the context of these new environments.

# Collective action and knowledge contribution in electronic networks of practice

MML Wasko, S Faraj, R Teigland

Year:2004

<https://aisel.aisnet.org/jais/vol5/iss11/15/>

## Abstract

Abstract  
Although there has been a significant increase in networked communication and a growing interest in virtual organizing, to date researchers have yet to establish consistent terminology and have paid little attention to how specific characteristics of the electronic network influence social dynamics such as knowledge contribution. To address this gap, we develop a theoretical model and a set of propositions that explain knowledge contribution in voluntary, computer-mediated, very large and open networks focused on knowledge exchange around a specific practice. We base our model on theories of social networks and collective action to explain how a social network of volunteers sustains productive exchanges between individuals, such as the exchange of knowledge. We utilize the concept of a network of practice to illustrate how the macrostructural properties of the communication media, network size, access to the network, and mode of participation affect network dynamics and knowledge contribution. We then develop a model and a set of propositions to suggest that knowledge contribution within an electronic network of practice is dependent upon 1) the macrostructural properties of the network, 2) the structure of ties that create the network, 3) the relational quality of ties that develop between individuals and the network as a whole, 4) the use of social controls, and 5) the distribution of individual motivations and resources in the network. We further predict that knowledge contribution influences the distribution of individual motivations and resources, as well as serves to create and recreate network structure over time. We conclude with a discussion of the implications of our theory for current and future research.

# Crisis in the IS Field? A Critical Reflection on the State of the Discipline

HK Klein

Year:2003

<https://aisel.aisnet.org/jais/vol4/iss1/10/>

## Abstract

Abstract  
This paper explores the issue of whether the field of IS is in crisis. To do so, the paper first starts by looking back on where the field has come from. Next, it assesses the status of the IS field by exploring where the field is now. That our current status remains a ¡®fragmented adhocracy¡¯ suggests the field may indeed be in crisis or headed for a crisis. This is compounded by the fact that there are two different views on the state of the IS field, each posing its own set of threats. One is the external view of the community (the view of IS from outside the academic field); the other is the internal view (the view from inside the IS community). By analyzing these two views, a better understanding of the problems the field faces emerges. In the next part of the paper, some thoughts are presented on where might the field go from here for overcoming its internal communication deficit. The paper proposes four different types of knowledge for structuring an IS Body of Knowledge (BoK) and following on from that, the value of creating a common BoK for the field. Lastly, the implications arising from the paper¡¯s analysis are explored. More specifically, the paper considers various options that are available for overcoming the internal communications deficit the IS field faces. These include changing the way the field thinks about generalizations, changing the institutional publication practices, focusing more on understanding the field¡¯s organizational stakeholders, and developing new knowledge creation and transformation networks. If IS as a field can overcome its internal communications deficits, it might ultimately contribute to the societal challenge of developing a deliberative cyber democracy and thereby help to address the social communication deficit which is a feature of modern mass societies.