Dec 12th, 12:00 AM

A Research Agenda to Understand Drivers of Digital Gullibility

Margeret Hall
Wirtschaftsuniversität Wien, margeret.hall@wu.ac.at

Christian Haas
Vienna University of Economics and Business (WU), christian.haas@wu.ac.at

A Research Agenda to Understand Drivers of Digital Gullibility

Short Paper

Margeret Hall
Vienna University of Economics and Business (WU)
Vienna, Austria
margeret.hall@wu.ac.at

Christian Haas
Vienna University of Economics and Business (WU)
Vienna, Austria
christian.haas@wu.ac.at

Abstract

Gullibility is a behavior set that includes insensitivity to cues signaling untrustworthiness, the propensity to accept false information, reject true information, or taking costly risks. It is a useful lens from which to view real-world adverse outcomes driven by the online behaviors of seemingly well-intentioned, or non-malicious, individuals. Though well established in pre-internet literature, gullibility has been largely sidestepped as a driver of adverse events in the digital era despite ample evidence for its existence. To better understand the drivers and contextual factors behind digital gullibility, we propose a comprehensive research agenda which aligns open research gaps with a set of research driven propositions. The agenda builds on existing models and discussions in related domains, structures open questions and provides guidance for IS researchers and practitioners in the face of ongoing digital gullibility.

Keywords: Digital gullibility, maladaptive outcomes, context collapse, network externalities

Introduction

Offline consequences of online information flows plague vulnerable users and systems (Pienta et al. 2016). Meanwhile, information systems' (IS) very ubiquity creates new and more frequent access points to those willing to accept false premises in the presence of untrustworthiness cues. Without gullible behaviors there could be no adverse outcomes from spam (Rao and Reiley 2012), phishing (Pienta et al. 2016; Sheng et al. 2010), or purchasing scams (Kitching 2017); (digital) misinformation flows (Ecker et al. 2022) would not generally lead to real-world political aggression (Fessler et al. 2017); and conspiracy theorists could not lead anti-vaccination campaigns at the risk of world-wide stability (Rodrigo et al. 2022). While the real-world existence of destabilizing digital affordances is irrefutable, currently we lack a theory that allows us to explain why such gullible behavior is happening, what the drivers are, and how IS can be designed to circumvent these outcomes. Into this gap we introduce a new theory of and research agenda for (digital) gullibility, experienced at the scale of the internet.

We suggest that the propensity to be 'duped' should be viewed as an input factor of maladaptive online behavior. However, the majority of IS research focuses on output functions like mis- and disinformation campaigns, cyber-attacks, or polarization. We view this akin to treating the symptoms rather than the disease. To remedy this knowledge and practice gap we need to understand which interaction effects between digitizing daily life and gullible behaviors exist and how gullibility may be an important driver of maladaptive outcomes linked to IS usage. Like this, we can move towards IS artifact design that supports individuals to understand and/or manage their gullible behaviors. We suggest that designing IS to support epistemic vigilance can improve outcomes for people and systems overall.

From the perspective of IS system design, we need a research agenda to better understand the drivers of digital gullibility in order to create resilient features for IS that can reduce, or even eliminate, the effects of digital gullibility and increase epistemic vigilance. This Work in Progress structures the remainder of the

paper as such: we introduce the underlying psychological constructs and intersections with IS from a socio-technical systems perspective. We then introduce two likely explanatory models, context collapse and network externalities. To design effective IS that acknowledge and mitigate gullible behavior and its antecedents, a better understanding of the drivers of gullibility is needed. Hence, we propose a research agenda for understanding and addressing digital gullibility based on three core research gaps intersecting gullibility and information systems research. We end with a research outlook.

Theoretical Basis

Gullibility, Credulity, and Trust

The constructs of credulity, gullibility, and trust are closely related. Credulity and gullibility differ at their actualization: Credulity is a belief characterized as the tendency to believe something without critically examining the evidence for that claim; gullibility is the corresponding behavior (Teunisse et al. 2020). Gullibility is typified by insensitivity to cues signaling untrustworthiness and the propensity to accept false information, reject true information, or take costly risks (Mercier 2017; Teunisse et al. 2020). It becomes maladaptive when expressed in the extreme: accepting or rejecting information such that there are negative or costly consequences. Intellectual deficits or age may play a role in having a higher propensity to accept false premises, but intellectual deficits and age are not a precursor to having credulous beliefs and/or engaging in gullible behaviors (Myers 2019; Sperber et al. 2010). Theory suggests that gullibility and trust are related (Rotter 1980). The two behaviors differ at an individual's willingness to accept untrustworthy cues in the presence of signals that other peers would not, meriting separate research consideration (Rotter 1980). While trust in internet transactions is well-addressed by theoretical and empirical research (Caton et al. 2012; Goldfarb and Tucker 2019), seminal works addressing gullibility tend to either sidestep the digital milieu (Laroche et al. 2019; Mercier 2017) or were first theorized and empirically tested before the widespread use of the consumer or social internet (Rotter 1980). Table 1 displays literature from psychology and IS addressing the constructs of trust, gullibility, and credulity and their considered information sources over time. Trust, misplaced trust, and gullibility towards social actors before the widespread use of the internet is well-addressed. Known organizational actors also somewhat covered in gullibility literature. Relationships between trust, gullibility, credulity and digital systems and agents are largely not addressed. The lack of convergence overall suggests a need for a targeted research agenda exists.

Author	Year	Construct			Information Source(s)					
					Social		Business		Technological	
		Trust	Gulli-bility	Cred-ulity	Kno wn	Un-known	Kno wn	Un-known	Kno wn	Un-known
Rotter	1980	X	X		X	(x)				
Yamagishi et al.	1999	X	X	(x)	X	(x)				
Greenspan	2008		X		X					
Sperber et al.	2010	X			X	(x)				
Pienta at al.	2016	X			X				X	(x)
Fessler et al.	2017			X		(x)				
Kitching	2017	X					X	X		
Mercier	2017		X		X	(x)				
Laroche et al.	2019	X	X				X			
Lin and Spence	2019	X					X		(x)	

Shen et al.	2019		X						X	(x)
Teunisse et al.	2020		X		X					
Balestrucci et al.	2021			X						X
Ecker et al.	2022	X			X					
Rodrigo et al.	2022	X			X					

Table 1. Psychological Constructs and Information Sources Investigated Over Time. X Indicates that the Concept is Covered; (x) Indicates that the Concept is Partially Covered.

There is an ongoing scholarly debate about the existence of gullibility. One literature strain based in psychology suggests that gullibility should not on average exist. From a theoretical basis we can expect that individuals learn from their behaviors and adapt to their (information) environments, indicating that if a gullible behavior would incur negative impacts, subsequent gullible behaviors would not occur (Mercier 2017). Two other theories from behavioral economics similarly argue against gullibility. One suggests that because individuals gain utility from maintaining a good image, they are unlikely to engage in behaviors which would harm that image (Akerlof and Kranton 2000), thus gullibility should not occur. Finally, the theory of rational inattention, whereby individuals incur negative outcomes due to lacking information, has been proposed as an alternative model to bridge assumptions of rationality and suboptimal information seeking and processing outcomes (Caplin and Dean 2015; Mackowiak et al. 2021).

Rational inattention and other existing theoretical models aim to explain suboptimal information seeking and verification behavior yet fail to fully explain why gullible behavior still occurs. Specifically, these theoretical lenses come up short in describing the occurrence of any given maladaptive behavior. The first two models rather portray gullibility as an impossible outcome given the underlying model assumptions. Rational inattention works well with the concept of epistemic vigilance, which is an individual's capacity to critically assess information (Sperber et al. 2010), but has a required fundamental assumption of individually rational behavior (Sims 2003). The degree to which gullibility can be linked to rationality, however, is unclear. Use of these models is unhelpful when trying to understand the many instances where users exhibit digital gullibility, through acting on obviously malicious, fake, or in general untrustworthy information, and for trying to understand how to build IS to support users and systems. We note an acute challenge exists in gullibility to social engineering operations. A theoretical model suggesting that gullibility does not on average exist but yet cannot explain the persistence of any given successful cybersecurity attack or misinformation campaign is at best not helpful and at worst actively harmful.

Applying a Socio-technical Systems Lens to Digital Gullibility

The use of socio-technical systems (STS) as a lens to understand how gullibility at scale became an issue helps clarify the reality of information processing behaviors as they exist today. STS enmesh people, tasks/processes, systems, technologies (Bostrom and Heinen 1977), and more recently, data (Weber et al. 2021). Ideally used in IS design and development stages (Scacchi 2004), STS still provides a useful theoretical framework for revising existing IS. STS advocates making people co-equals in design and development of IS, which is often overlooked in practice (Bostrom and Heinen 1977). We point out a flawed assumption of how individuals (*people*) will use the internet (*technological systems*) as a first failure point; a common criticism from the STS lens. Since the 1960's it was recognized as a logical fallacy that one must not understand how an information system works (*tasks/processes*), only how to use it (Ackoff 1967). Simply plugging individuals into the internet without further resources and training on how to best search for information (*data*) or indeed their own epistemic vigilance, has proven insufficient, leading to the content and practices of the internet as it stands now: searching, trusting, and using an *a priori* unknown mixture of information ranging between very high and very low quality (Metzger et al. 2015; Yamamoto and Yamamoto 2018).

A first necessity to understand digital gullibility then is addressing the degree to which *people* interact with and in information-based digital *technological systems*. Figure 1 models and extends 'people' and their interactions as theorized by (Heide and Wathne 2006). We can expect that individuals have social and business exchanges in person and digitally. Extending this, we should not neglect the role of fully digital agents like bots on the internet. Bots are quasi-social communication agents which can also be a source of influence on the internet (Balestrucci et al. 2021). Moreover, (Heide and Wathne 2006) assumed that exchanges are based on mostly-known interlocutors. On the internet this cannot be assumed (Caton et al. 2012; Goldfarb and Tucker 2019); IS are designed to facilitate exchanges in social and commercial scenarios regardless of the familiarity level, meaning this is the norm instead of the exception.

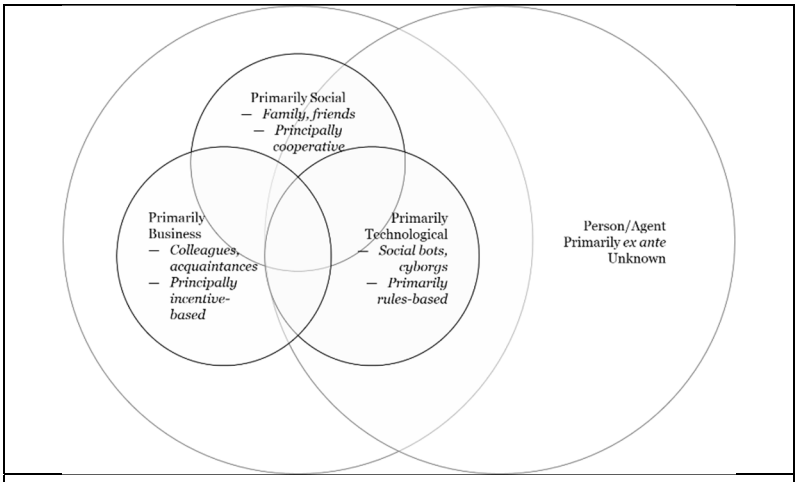

Figure 1: Extending Heide and Wathne (2006) into Role-based Sources and Context of Information

Tasks and processes on the internet are fundamentally *n* to *n* or *n* to *m* exchanges of *data*, facilitated by the underlying *technology*. The *structure* is the collection of formal and informal rules of use, ranging from community moderation guidelines and Terms and Conditions to the legislative environment. The interaction effect creates the internet and its bright and dark sides as it is known today and allows for a theoretical nesting of the digital environment whereby gullibility is demonstrated.

STS alone is not a behavioral model and does not elucidate potential drivers of gullibility, but rather can demonstrate how individual gullibility can manifest itself and be exploited on the internet. Building on this, we propose to investigate two models which integrate the STS perspective as explanatory cases for the persistence of suboptimal outcomes linked to online gullibility. First, context collapse (Shen et al. 2019; Vitak 2012) is promising as it addresses the burden of individually validating digital information. Validating quality and trustworthiness of known and unknown agents including social contexts, business contexts, and artificial agents is a significant cognitive burden and may be a reason why digital gullibility continues to plague IS users. Second, by viewing gullible behaviors in the context of accountability and network externalities. Considering the perspective of Mercier (2017), individuals will discontinue gullible behaviors because they learn from the consequences. What happens when there are no or few consequences borne by the individual? Both the learning function necessary to stop gullibility would be missing, and if changing one's own behavior to reduce or avoid future gullible behavior would incur costs, it would in fact disincentivize the individual to change their behavior. (Hill et al. 2020).

To better understand the relevance of these potential drivers of digital gullibility, we integrate them into a holistic research agenda for understanding digital gullibility. This research agenda will help to shed light on contexts, drivers, and prevalence of digital gullibility and investigate if context collapse and/or network externalities can explain gullible behavior.

A Research Agenda to Understand Digital Gullibility

We base our proposed research agenda on two foundational works to link gullibility and information seeking behavior. First, from a psychology perspective researchers investigated different aspects that are protective against gullible behavior, presenting evidence of epistemic vigilance based on effective mechanisms for analyzing communicated information (Mercier 2017; Sperber et al. 2010). In our research agenda, we plan to investigate which mechanisms of epistemic vigilance exist for users in IS, and how they depend on characteristics of the information (e.g., perceived value or the information source). Second, individual user characteristics generally influence the degree of information seeking behavior in IS (Johnson 2003). As information seeking and verification is a crucial strategy to estimate trustworthiness, we propose investigating the relevance of user characteristics on information seeking and verification behavior in situations of heterogeneous (un)trustworthy information. Finally, in addition to (potentially context-specific) epistemic vigilance and individual information seeking behavior, we investigate the relevance of additional antecedents of an intent to act on (potentially harmful) information. Specifically, the research agenda considers questions of network externalities, i.e., misplaced accountability of a user's actions, and its effect on observed gullible behavior.

Taken together, Figure 2 presents a proposed model and research agenda that considers antecedents, interactions, and influences on gullible behavior. To better structure the research agenda into its different components, we suggest a proposition-driven agenda by splitting the overall agenda into specific research gaps and propositions, i.e., aggregate different questions and propositions into groups for model development and confirmation. Next, we provide more details on the specific research gaps by defining central propositions in the respective groups.

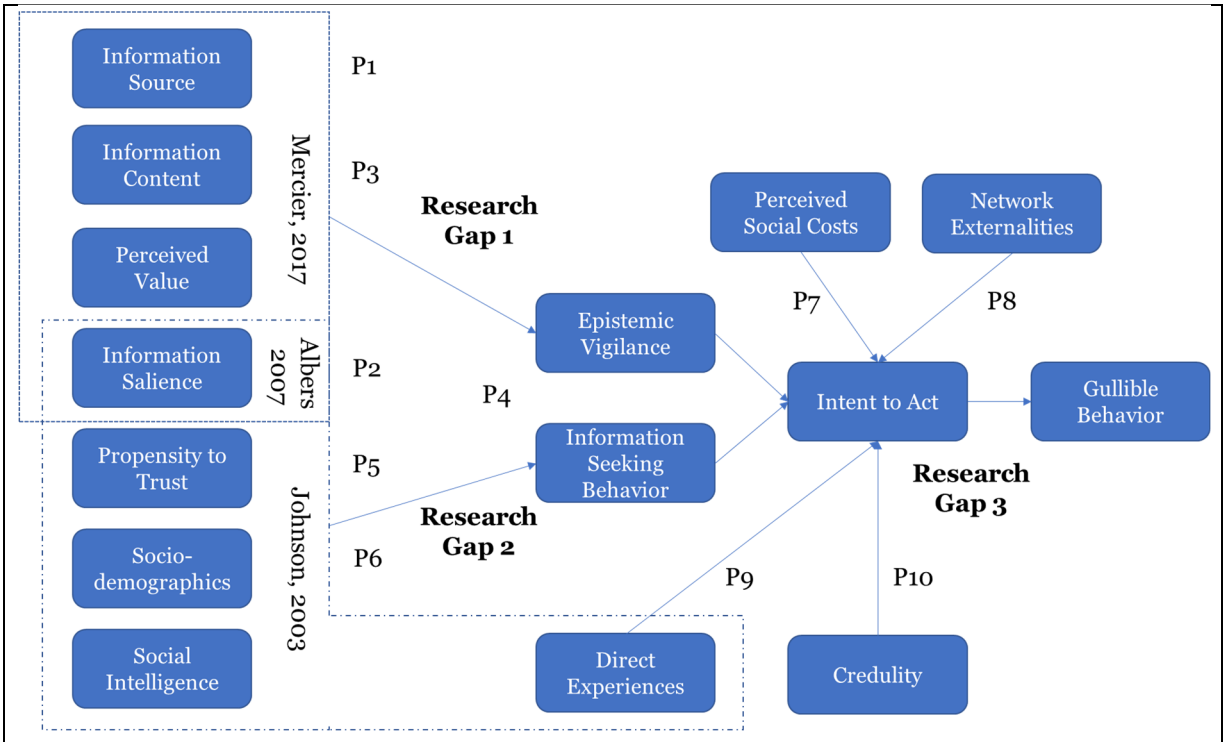

Figure 2: Research Agenda and Research Gaps for Understanding Digital Gullibility

Research gap 1: Information context and potential context collapse

The first research gap considers the impact of information characteristics on an individual's (i.e., system user's) epistemic vigilance. Epistemic vigilance here refers to the mental and/or cognitive evaluation and discrimination of a given information type and/or source (Sperber et al. 2010). Mercier (2017) identified several influencing factors attributed to protecting against gullibility. Research gap 1 aims to further our

understanding of the relevance of these potential protective factors in the setting of digital information and IS. We focus on the following three core propositions for research gap 1.

P1: Established trust in an information source decreases epistemic vigilance.

As mentioned before, trust is an essential part of (digital) information systems yet can be dangerous if trust is placed in malicious information (Pienta et al. 2016; Rotter 1980). This proposition considers how epistemic vigilance is affected based on user's experiences and prior interactions with different types of information sources and the resulting level of trust, from differing agent types to familiarity levels.

P2: Higher information salience increases epistemic vigilance.

Not all information is relevant to evaluate (mis)information, and too much information can lead to information overload. Hence, information recipients can be queued to focus on the most salient pieces of information (Albers 2007). However, this could also lead to users focusing on the most salient information, which might be correct, and disregard the potentially incorrect, less salient pieces of information. Proposition 2 investigates how epistemic vigilance is affected by the salience of an information source.

P3: Information content and its perceived value affects individual's epistemic vigilance.

Gullible behavior and spreading misinformation can depend on the type of information content and its value (Mercier 2017). For example, users might exhibit higher baseline vigilance in business information systems when being confronted with (potentially fake) invoices or requests from potential business partners compared to news, rumors, or personal information shared in private social networks. Hence, proposition 3 investigates the dependency of epistemic vigilance on the specific content of the information.

Taken together, research gap 1 aims to investigate and clarify drivers of epistemic vigilance, i.e., drivers of (misplaced) trust in specific information sources and content. Addressing this research gap will allow for a proactive management of different information types in IS by managing the epistemic vigilance of users.

Research gap 2: Individual characteristics for information seeking behavior

Research gap 2 considers the impact of information seeking and verification behavior on gullible actions. Depending on the type of information a user is exposed to and the required costs and effort to pursue information verification, users might engage in a range of different information seeking and verification efforts (Vitak 2012; Yamamoto and Yamamoto 2018). The goals of this research gap are to better understand the drivers of information seeking behavior for (un)trustworthy information and to identify salient factors for it. Ultimately, future IS should encourage users to engage in information verification while keeping the required costs and efforts as small as possible (Goldfarb and Tucker 2019; Maertens et al. 2020).

P4: Context collapse decreases epistemic vigilance and information seeking behavior.

In case of many different information sources, maintaining separate expectations of trustworthiness for each source puts a high cognitive load on users. This can lead to users following a cognitive heuristic such as context collapse, the flattening and equalizing of multiple distinct information sources into (trustworthy) monoliths at scale (Vitak 2012). Such a cognitive heuristic can lead to gullible behavior if trust is misplaced. However, this might also depend on previous experiences with similar types of information, the value and source of the shared information, and socio-demographic factors of the user.

P5: The effort of information verification and seeking decreases with an individual's propensity to trust in an information source.

Previous work showed that individuals place a different level of trust in information and different information sources (Caton et al. 2012; Lin and Spence 2019; Yamagishi et al. 1999). Higher trust, e.g., based on a better reputation of an information source, generally leads to lower information verification costs and efforts (Goldfarb and Tucker 2019). This proposition centers around the impact of information seeking and verification effort on an individual's propensity to trust.

P6: Socio-demographic characteristics influence information seeking behavior.

As mentioned earlier, gullible behavior historically was linked to highly vulnerable communities as a symptomatic trait of mental disability, or the very young or old (Greenspan 2008), yet evidence suggests that such behavior can be observed across a range of different users (Maertens et al. 2020; Shen et al. 2019). Hence, additional research is needed to identify the impact of socio-demographic factors on information seeking and verification behavior and ultimately also gullible behavior. While socio-demographic factors might be used as control variables in the other propositions, they can be considered moderating or independent variables here due to their key importance on the hypotheses for this proposition.

Research gap 3: Realized Gullible Behavior and Network Externalities

Building on the previous two research gaps, gap 3 investigates the concrete impacts that the identified drivers, consequences, and information characteristics have on realized gullible behavior. From a decision-making perspective, we propose to view and study realized gullible behavior through the lens of (micro-) economic models where individuals receive utility from (acting on) information and incur costs from potential consequences (e.g., verification costs, image costs, etc.).

P7: An individual's perception of (social) costs for acting on information influences the propensity to engage in gullible behavior.

Previous research, including models using image utility which suggest that users derive utility from how they are perceived by others, suggest that users who value their perception by others should not engage in gullible behavior (Akerlof and Kranton 2000). The first proposition in gap 3 investigates if and how gullible behavior is a function of the perceived social costs (as a change in perception) from acting on information.

P8: Higher costs of consequences for acting on information decrease the frequency of gullible behavior.

Acting on malicious information may come with consequences, ranging from no consequences at all up to extreme costs such as potentially being liable for damages incurred by acting on malicious information. Generally, following decision making models such as (Mackowiak et al. 2021; Mercier 2017) we should expect that higher expected costs from gullible behavior decreases the frequency of such behavior in users, subject to contextual factors such as the specific information system and the type of information shared. Likewise, consequences that are distributed across groups e.g., a successful phishing attack occurs via a single email account but impacting operations across an institution, as opposed to solely borne by the gullible individual, may not directly dissuade from future gullible behavior.

P9: Previous direct experiences with an information source and information content influence the intent to act and gullible behavior.

An individual's utility can also be dependent on perceived norms, e.g., based on prior experiences with specific information. A norm in the context of malicious information can be the perceived trustworthiness, or respectively the perceived maliciousness, of specific information (Bordalo et al. 2020). This proposition considers the impact of novelty on a user's propensity to engage in gullible behavior. On the one hand, if a user is exposed to certain information for the first time, the propensity of gullible behavior might be higher due to uncertainty in establishing the trustworthiness of the information content or source. On the other hand, previous experiences can also be strategically used against users who misplace trust. For example, given previous positive experiences with a specific information content and/or source a user might perceive it as trustworthy, and a creator of malicious information can use this to ultimately send malicious information later once user trust has been established.

P10: Propensity of gullible behavior depends on an individual's level of credulity.

While previous research suggests that individual users have different baseline levels of credulity (Balestrucci et al. 2021), we do not know if this level of credulity also depends on the type of information and/or the context in which the information is consumed. This proposition aims to further understand the drivers of individual credulity and its effects on realized gullible behavior.

Summary and Outlook

Digital gullibility and its effects can be observed in many information systems, yet its potential drivers are theoretically under-addressed. Due to the prevalence of adverse outcomes in the real world driven by gullible behavior online, we propose a research agenda to investigate the phenomenon of digital gullibility. The agenda proposes the use of STS to understand how gullibility can impact digital behaviors and opens questions on the explanatory value of context collapse and network externalities as behavioral models. The research agenda structures open questions and provides guidance for researchers who aim to investigate aspects of digital gullibility. Addressing the research agenda will provide useful information on the drivers of gullible behavior and their dependency on content, context, and user demographics. From an IS perspective, the agenda will enable IS designers to reduce the occurrence of gullible behavior in information systems and to mitigate its effects. Similar to mitigation approaches to increase fake news resilience (Maertens et al. 2020; Rodrigo et al. 2022), this can include user-centric solutions to increase awareness of the most important drivers of digital gullibility (e.g., context collapse and network externalities), system elements that reduce information verification costs, or data-driven AI and ML solutions that provide suggestions about the likelihood of information trustworthiness.

As immediate next steps, we plan to address the proposed research gaps by developing more detailed hypotheses for the propositions, followed by a detailed research design utilizing theoretical modeling, user experiments, and empirical analysis. Theoretical online user behavior modeling, e.g., based on micro-economic and game-theoretic approaches, can yield important insights into expected behavior, whereas user experiments and empirical analysis can shed further light on realized gullible behavior and potential gullibility drivers in specific contexts.

References

Ackoff, R. 1967. "Management Misinformation Systems," Management Science (14:4), pp. 146–156.

Akerlof, G. A., and Kranton, R. E. 2000. "Economics and Identity," The Quarterly Journal of Economics (115:3), pp. 715–753.

Albers, M. J. 2007. "Information Salience and Interpreting Information," SIGDOC'07: Proceedings of the 25th ACM International Conference on Design of Communication, pp. 80–86.

Balestrucci, A., De Nicola, R., Petrocchi, M., and Trubiani, C. 2021. "A Behavioural Analysis of Credulous Twitter Users," Online Social Networks and Media (23), Elsevier B.V., p. 100133.

Bordalo, P., Gennaioli, N., and Shleifer, A. 2020. "Memory, Attention, and Choice," Quarterly Journal of Economics (135:3), pp. 1399–1442.

Bostrom, R., and Heinen, J. S. 1977. "MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes," MIS Quarterly (1:3), pp. 17–32.

Caplin, A., and Dean, M. 2015. "Revealed Preference, Rational Inattention, and Costly Information Acquisition," American Economic Review (105:7), American Economic Association, pp. 2183–2203.

Caton, S., Dukat, C., Grenz, T., Haas, C., Pfadenhauer, M., and Weinhardt, C. 2012. "Foundations of Trust: Contextualising Trust in Social Clouds," in Proceedings - 2nd International Conference on Social Computing and Its Applications, CGC/SCA 2012, pp. 424–429.

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K., and Amazeen, M. A. 2022. "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction," Nature Reviews Psychology (1:1), Nature Publishing Group, pp. 13–29.

Fessler, D. M. T., Pisor, A. C., and Holbrook, C. 2017. "Political Orientation Predicts Credulity Regarding Putative Hazards," Psychological Science (28:5), pp. 651–660.

Goldfarb, A., and Tucker, C. 2019. "Digital Economics," Journal of Economic Literature, pp. 3–43.

Greenspan, S. 2008. "Foolish Action in Adults with Intellectual Disabilities: The Forgotten Problem of Risk-Unawareness," International Review of Research in Mental Retardation (36th ed.), (L. M. Glidden, ed.), New York: Elsevier, pp. 147–194.

Heide, J. B., and Wathne, K. H. 2006. "Friends, Businesspeople, and Relationship Roles: A Conceptual Framework and a Research Agenda," Journal of Marketing (70:3), SAGE Publications.

Hill, R., Stein, C., and Williams, H. 2020. "Internalizing Externalities: Designing Effective Data Policies," AEA Papers and Proceedings (110), American Economic Association, pp. 49–54.

Johnson, J. D. 2003. "On Contexts of Information Seeking," Information Processing & Management (39:5), Pergamon, pp. 735–760.

Kitching, T. 2017. Purchasing Scams and How to Avoid Them, (1st ed.), London: Routledge.
Laroche, H., Steyer, V., and Théron, C. 2019. "How Could You Be So Gullible? Scams and Over-Trust in Organizations," Journal of Business Ethics (160:3), pp. 641–656.
Lin, X., and Spence, P. R. 2019. "Others Share This Message, So We Can Trust It? An Examination of Bandwagon Cues on Organizational Trust in Risk," Information Processing and Management (56:4), Elsevier Ltd, pp. 1559–1564.
Mackowiak, B., Matejka, F., and Wiederholt, M. 2021. "Rational Inattention: A Review," No. 2570, Frankfurt a. M. (https://www.econstor.eu/bitstream/10419/237709/1/ecb.wp2570.pdf).
Maertens, R., Roozenbeek, J., Basol, M., and Van Der Linden, S. 2020. "Long-Term Effectiveness of Inoculation Against Misinformation: Three Longitudinal Experiments," Article in Journal of Experimental Psychology Applied.
Mercier, H. 2017. "How Gullible Are We? A Review of the Evidence from Psychology and Social Science," Review of General Psychology (21:2), pp. 103–122.
Metzger, M. J., Flanagin, A. J., Markov, A., Grossman, R., and Bulger, M. 2015. "Believing the Unbelievable: Understanding Young People's Information Literacy Beliefs and Practices in the United States," Journal of Children and Media (9:3), pp. 325–348.
Myers, D. G. 2019. "Psychological Science Meets a Gullible Post-Truth World," in The Social Psychology of Gullibility: Conspiracy Theories, Fake News and Irrational Beliefs, Routledge, pp. 77–100.
Pienta, D., Sun, H., and Thatcher, J. 2016. "Habitual and Misplaced Trust: The Role of the Dark Side of Trust Between Individual Users and Cybersecurity Systems," in ICIS 2016 Proceedings, December 11.
Rao, J. M., and Reiley, D. H. 2012. "The Economics of Spam," Journal of Economic Perspectives (26:3), pp. 87–110.
Rodrigo, P., Arakpogun, E. O., Vu, M. C., Olan, F., and Djafarova, E. 2022. "Can You Be Mindful? The Effectiveness of Mindfulness-Driven Interventions in Enhancing the Digital Resilience to Fake News on COVID-19," Information Systems Frontiers (1), Springer, pp. 1–21.
Rotter, J. B. 1980. "Interpersonal Trust, Trustworthiness, and Gullibility," American Psychologist (35:1), pp. 1–7.
Scacchi, W. 2004. "Socio-Technical Design," The Encyclopedia of Human-Computer Interaction, (W. S. Bainbridge, ed.), Berkshire Publishing Group.
Shen, T. J., Cowell, R., Gupta, A., Le, T., Yadav, A., and Lee, D. 2019. "How Gullible Are You? Predicting Susceptibility to Fake News," in WebSci 2019 - Proceedings of the 11th ACM Conference on Web Science, Association for Computing Machinery, Inc, June 26, pp. 287–288.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010. "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in Conference on Human Factors in Computing Systems - Proceedings (Vol. 1), ACM, pp. 373–382.
Sims, C. A. 2003. "Implications of Rational Inattention," Journal of Monetary Economics (50:3), North-Holland, pp. 665–690.
Sperber, D., Clément, F., Heintz, C., Mascaro, O., Mercier, H., Origgi, G., and Wilson, D. 2010. "Epistemic Vigilance," Mind & Language (25:4), John Wiley & Sons, Ltd, pp. 359–393.
Teunisse, A. K., Case, T. I., Fitness, J., and Sweller, N. 2020. "I Should Have Known Better: Development of a Self-Report Measure of Gullibility," Personality and Social Psychology Bulletin (46:3), pp. 408–423.
Vitak, J. 2012. "The Impact of Context Collapse and Privacy on Social Network Site Disclosures," Journal of Broadcasting & Electronic Media (56:4), pp. 451–470.
Weber, M., Hacker, J., and Vom Brocke, J. 2021. "Resilience in Information Systems Research-A Literature Review from a Socio-Technical and Temporal Perspective," in ICIS 2021 Proceedings.
Yamagishi, T., Kikuchi, M., and Kosugi, M. 1999. "Trust, Gullibility, and Social Intelligence," Asian Journal of Social Psychology (2:1), John Wiley & Sons, Ltd, pp. 145–161.
Yamamoto, Y., and Yamamoto, T. 2018. "Query Priming for Promoting Critical Thinking in Web Search," CHIIR 2018 - Proceedings of the 2018 Conference on Human Information Interaction and Retrieval (2018-March), pp. 12–21.