The Interplay between Human and Machine Agency

J. Brian Pickering, Vegard Engen and Paul Walland

IT Innovation Centre
Gamma House, Enterprise Road
Southampton, SO16 7NS, UK
{jbp,ve,pww}@it-innovation.soton.ac.uk

Abstract. Human-machine networks affect many aspects of our lives: from sharing experiences with family and friends, knowledge creation and distance learning, and managing utility bills or providing feedback on retail items, to more specialised networks providing decision support to human operators and the delivery of health care via a network of clinicians, family, friends, and both physical and virtual social robots. Such networks rely on increasingly sophisticated machine algorithms, e.g., to recommend friends or purchases, to track our online activities in order to optimise the services available, and assessing risk to help maintain or even enhance people's health. Users are being offered ever increasing power and reach through these networks by machines which have to support and allow users to be able to achieve goals such as maintaining contact, making better decisions, and monitoring their health. As such, this comes down to a synergy between human and machine agency in which one is dependent in complex ways on the other. With that agency questions arise about trust, risk and regulation, as well as social influence and potential for computer-mediated self-efficacy. In this paper, we explore these constructs and their relationships and present a model based on review of the literature which seeks to identify the various dependencies between them.

Keywords: General: HCI methods and theories · Human-machine networks · Agency · Trust · Modelling · Self-efficacy

1 Introduction

A definition of agency based on the notion of non-deterministic behaviours [1] fails to recognise the increasing variety and complexity of human-machine networks [1] (HMNs) [2], the intention of technology designers [3], and active intervention by bots within social networks [4, 5]. The concept of agency is particularly problematic in human-machine interactions [6]. Machine or material agency may be seen as automation, which originally required some tolerance from human agents [7]. But this is no longer true: technology can actively support human activity [8], and manifests increasingly complex interaction types [9]. Machine and human agency may not be the same and yet equally valid [10]; machine agency may be just "perceived autonomy" [11]; and it

---

[1] In the following we use *human-machine network* and *network* interchangeably.

certainly enables human agency [12]. Indeed, agency may well be becoming a social and group construct where both humans and machines play a part [13, 14]; and used effectively, agency may even lead to innovative review of working practice [15].

The enabling contribution of machine agents within a network may have an effect on self-efficacy. Bandura's original definition of self-efficacy as an individual's belief in their ability to be able to achieve a given objective [16–18] has also been applied to technology [19, 20] and its acceptance [21]. There are, however, constraints on the support and positive contribution of technology to human self-efficacy, not least in terms of anxiety and suspicion around technology use [22, 23]. This may be further exacerbated by increasing machine animism: it may not always be obvious what machines are doing or what information they are collecting on other agents in the network [24, 25]. With this in mind, regulation is seeking to impose safeguards [26], but with only limited success [27]. Any consequent perception of risk can undermine a willingness to engage in some online activities [28]. However, assuming scepticism can be kept low, regulation can reduce the negative effects of risk across a number of contexts, leading to an increased level of trust [29].

Bringing together some of these constructs, this paper proposes updates to a recent model of trust in information technology [30, 31] with a detailed exploration of self-efficacy as it relates to agency [3, 18]. Since human-machine networks can be characterised by independently varying levels of agency [2], either or both may influence self-efficacy [18]. Further, introducing regulation and perceived risk [32], how these influence agency and, in turn, behaviours within an HMN, need consideration [33, 34]. On the other hand, for this exploratory study, we do not consider affect [35] or other motivators such as social identity or task [36] which may mediate behaviour in online networks. Similarly, we discount environmental trust as factors affecting both behaviour and self-efficacy [37].

In the original study by Thatcher et al. [31], the final set of constructs was based on an extensive literature review [30], and its validation via an opportunity sample of students and IT professionals to establish inter-construct dependencies and correlations. The intent to explore technology was seen to be dependent on social norms and computer self-efficacy, while the influence of trust in IT and in support personnel is mediated by the technology acceptance model (TAM) constructs of perceived usefulness and ease of use. The relationship between interpersonal, organisational and technology trust is well motivated in light of theoretical considerations of trust transfer [38], and of trust as an overall organising factor [39]. However, given the various interactions between agents within an HMN, both human-to-human and machine-to-machine, the question remains whether McKnight et al. [30] had captured all relevant constructs. Further, participants were drawn from a narrow field who may show a priori increased propensity to engage and persevere with technology [40]. Revisiting and extending their original model with specific reference to HMNs, therefore, implies careful consideration of those constructs as well as participant selection in validating the resulting research model.

2 Modelling Trust

Interpersonal and person-to-organisation trust is based on the judgement of perceived benevolence, integrity and competence [41, 42]. More recently applied to technology and its acceptance, self-efficacy and agency in HMNs interact with one another as well as influence trust. It is, therefore, appropriate to reconsider a model of trust in online interactions.

2.1 Related Research

In a series of studies McKnight, Thatcher and their colleagues explored different constructs associated with trust in technology [30, 31]. They found that trust in technology and a willingness to explore its use could be predicted from individual propensities to trust. Further, context-specific factors including social context and an individual's computer self-efficacy were found to relate directly to this willingness to explore technology [31].

Other studies, however, highlight a range of different constructs. For example, an extensive literature review suggests personal, organisational as well as cultural factors as instrumental for online trust [43]. Many studies stress the social [44, 45], not least the importance of communication and group adherence [46] and self-efficacy [37]. However, this social dimension is closely connected with agency [47]. Still others explore the interplay of risk, assurances of privacy and security [29, 48]. Drawing all of this together suggests an extension to the Thatcher et al model to incorporate greater focus on the social on the one hand, but also regulation and risk perception on the other.

2.2 Research Model

The focus of the proposed research model is human behaviour in an HMN. For an HMN to be successful, and both gain and sustain participation, it needs to enable benefits for the human agents within the network. Although there are a number of human participants taking different roles, it may well be that the network benefits one group in a different, or preferential, way to others. This does not alter the fact that the network, and the machine agents within it, are established in order to provide benefit to the human actors in that network.
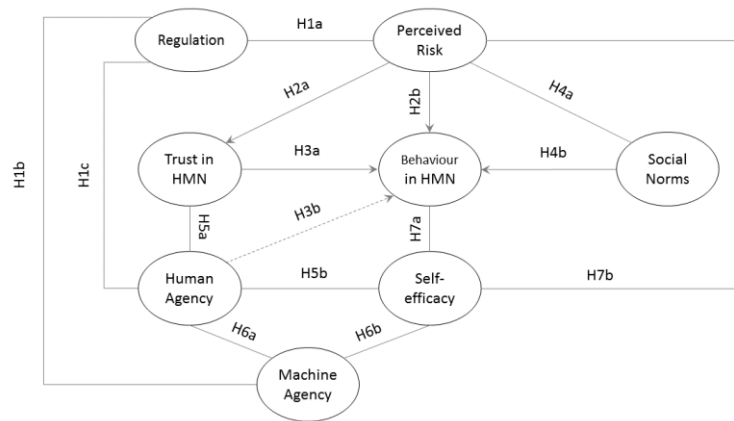
Fig. 1. Research Model

We are concentrating on human behaviour in the HMN, rather than human actions. This is an important distinction, since, as has been discussed elsewhere [49], human actors exhibit 'conscious intentionality', which is to say that the human actors have certain freedom of choice regarding their actions, whereas the machine agents exhibit 'programmed intentionality' in the sense that they can also influence behaviour, but do so according to their pre-determined programming and rule sets [50]. How a human behaves in a particular network and circumstance will depend upon a number of factors acting upon them, which are reflected in **Fig. 1**.The main proposition is that a human agent will behave in a manner which is determined by two considerations: their belief that they can achieve what they want in the network (self-efficacy) [16–18] and the level of risk that they perceive in performing those actions (trust) [28, 29]. What other constructs should be included is the purpose of this section.

First, we introduce the effect of regulation on agency, since regulation, whether legislative, standardisation or commercial restriction, will set limits on both machine agency and human agency [32]. Another effect of regulation is to modify the perceived risk involved in performing actions, positively or negatively [26, 32]. We identify perceived risk rather than actual or absolute risk, because it is perceived risk that determines human behaviour, not the actual level of risk, as established in a broad spectrum of research, including inter alia online consumer behaviour [51, 52], health care [53], and engineering and natural disasters [54]. For example, vanishingly rare events such as the murder of a child affect parents' perception of risk to their child, even though the actual risk is very small, and lower than the risk of injury at home. Thus, anything that modifies perceived risk is important, even if the actual level of risk is unchanged. We can, therefore, also conclude that trust is a reflection of perceived risk, and that behaviour is a reflection of willingness to accept a certain level of risk, both of which are based on belief, not on absolute or measurable parameters [31, 55]. Risk perception,

trust and behaviour can all change with time, and can be modified by changes in circumstance, such as external influences (social norms) [56, 57].

Behaviour is also determined by ease of use of the network, expressed as ability to achieve pre-determined goals (self-efficacy). Machine agency can operate in a supportive role, enabling ease of use and hence supporting self-efficacy [50], leading to more positive or interactive behaviour and better achievement of objectives by the human agent. Limitations to the supportive ability of the machine agent, either through regulatory limitations or functional limitations, may reduce the self-efficacy they can support, leading to more cautious behaviour [31]. This would suggest an association with perceived risk: belief in one's own capabilities and therefore the ability to manage perceived risks.

3 Model Constructs and Research Hypotheses

As the central construct of our model, Human Behaviour in HMN[2] is affected directly or indirectly by all of the remaining constructs. In consequence, we have developed hypotheses for all the remaining constructs in the following sections. These will determine relationships with behaviour in HMN.

3.1 Regulation

We include laws (legislations), codes of practice and standards as part of this construct. As discussed above, regulations may constrain agency. It may also have enabling effects, such as technology standards improving on technology interoperability and ensure security and privacy for end-users [58], which are all key to HMNs dealing with personal data. Standardisation efforts, such as HL7 in healthcare[3], may, therefore, have a positive impact on both human and machine, as well as reducing the perceived risk. Miltgen and Smith [32] have already shown that higher levels of perceived regulatory protection is associated with a decrease in the risks that people perceive to their privacy. In this vein, we hypothesise the following.

H1a: Perceived risk is negatively correlated with changes in regulation.

However, regulation may also stifle innovation and constrain what actors are allowed to do, directly reducing both human and machine agency[4]. Reasons for regulations to be constrictive may be to, e.g., address concerns regarding the increasing autonomy of machines [2], raising ethical issues about responsibilities and accountability [59]. Thus, we hypothesise:

H1b: Machine agency is negatively correlated with increasing levels of regulation.

---

[2] Abbreviated to "Behaviour in HMN" in the remaining discussion
[3] HL7 – Health Level Seven. http://www.hl7.org.uk/
[4] EC H2020 SHiELD Project, 2017, http://cordis.europa.eu/project/rcn/207185_en.html

In the discussion above, we can see that the effect on human agency can vary, depending on the increase in regulations. On the one hand, it may increase human agency due to the reduction in the perceived risk (via trust in the HMN, as discussed further below). On the other hand, it may decrease human agency due to the reduction in machine agency, as hypothesised above. Therefore, we simply put forth the following hypothesis:

H1c: Regulation affects human agency.

3.2 Perceived Risk

The perception of risk and uncertainty was considered by Thatcher et al. [31], but was omitted from their proposed model. Here, we focus on the perception of risk as experienced by the human participants in an HMN. However, we do note that this also affects other actors, such as providers and even machines although their response is deterministic. While exploring the different types of risk that could affect trust and the behaviour of participants in an HMN is outside the scope of this paper, this could include any factors of an HMN pertaining to, e.g., monetary loss or loss of privacy, as discussed in [32, 60]. We focus here on the perception of risk experienced when participating in HMNs, which may well differ from actual risk as discussed above; the former affecting behaviour [31, 55], which pertains to the central construct we are interested in here (Behaviour in HMN). Pavlou [60], in proposing extensions to the TAM, found that trust influences perceived risk. Here we focus on how perceived risk affects trust in the HMN, leading to the following hypothesis:

H2a: The perception of risk negatively affects trust in an HMN.

While previous work, as discussed above [55, 60, 61], establishes that trust affects the perception of risk, we also hypothesise a direct relationship between Perceived Risk and Behaviour in HMN.

H2b: The perception of risk negatively affects the behaviour in an HMN.

3.3 Trust in HMNs

As a construct, trust pervades almost all interactions between individuals and is traditionally the result of perceived benevolence, competence and integrity [41]. Over time, it may be lost but also rebuilt [42], largely due to context and reassessment of behaviours and intention. If trust is an overall organising principle [39], then it makes sense to attempt to extend the construct to technology [30] and online networked activities [38]. So trust will affect self-efficacy [31, 37] and be associated with social norms [31]. It may well be that interpersonal and technology trust differ in the detail, but collectively influence a willingness to adopt the technology [62]. Once online, traditional behaviours occur: communication is important [46], and social trust will affect willingness to engage [63]. Further, increasing familiarity with the technology may well influence trust and thereby agency [20, 30], though there will be a moderating effect in relation to security risk or privacy exposure [48]. We therefore hypothesise that:

H3a: HMN trust will positively influence the behaviour in an HMN.

further

H3b: HMN trust will mediate human agency and the behaviour in an HMN.

3.4   Social norms

A significant research body on social norms in the offline world is gradually being extended into the virtual world, already finding parallels even down to eye gaze and social gestures [64] and group composition [65]. A willingness to engage online involves social pressures from the immediate social group, social identity [66] and trust in other network members [63]. Indeed the desire to be seen online will often motivate the adoption of strategies to mitigate against potential risk [56, 57], or even adapt structures such as reputation and social presence in decisions to engage, for instance in eCommerce [67]. Along with (computer) self-efficacy, social norms may also influence participation in social networks [68], and even encourage emergent and shared agency within the virtual group [13]. Thatcher et al. [31] were clearly right to include social norms in their model, though they did not necessarily explore the full implications of its influence. Specifically, social norms can reduce perceived risk, as well as directly encourage online engagement and behaviours. In consequence, we propose that:

H4a: Social norms will affect the extent to which perceived risk influences the behaviour in an HMN.

and

H4b: Social norms will directly and positively correlate with the behaviour in an HMN.

3.5   Human agency

A pragmatic definition of Human and Machine Agency in HMNs has been discussed in [3] on the basis of a review of social psychology literature, such as Structuration Theory [61] and Social Cognitive Theory [49]. Adopting the definition of agency from [3] we understand agency "as the capacity to perform activities in a particular environment in line with a set of goals/objectives that influence and shape the extent and nature of their participation". In practice, agency, therefore, indicates what a human actor can actually do in the network, and how this aligns with the objectives they would have for using the network, or their belief in their ability to achieve their goals. This, in turn, influences their behaviour in the network. We hypothesise a direct relationship between human agency and self-efficacy in terms of the behaviour in the HMN, as follows:

H5a: Trust in the HMN is positively correlated with human agency.
H5b: Human agency is related to self-efficacy.

3.6 Machine agency

As per [3], we can apply the same definition for Human Agency, as discussed above, to Machine Agency. While there are distinctions between the two, such as the lack of intentionality in machines [69, 70], they are increasingly active and visible participants in HMNs, even exhibiting human-like characteristics, capable of exerting influence and enhancing Human Agency [3]. The latter is due to a characteristic that Bandura [49] refers to as proxy agency, in which an agent may increase their own agency by utilising the capabilities of other agents, which could indeed be machines. However, it is far from clear whether machine agency might be perceived as a constraint on human activity itself or in overall processes [15]. Similarly a unidirectional relationship may not hold: human agency may well constrain machine agency if this means that human agents simply do not need the full capabilities of machines. Indeed, Følstad et al. [59] indicate a bi-directional and synergistic relationship, which warrants further exploration. Thus, we pose the following generic hypothesis:

H6a: Machine agency in an HMN is directly related to human agency.

The nature of this relationship may need more careful consideration. A similar issue arises regarding the relationship between Machine Agency and Self-efficacy, confounded by factors such as the age and cultural background of those engaging in the HMN. Whilst increasing machine agency may indeed increase the self-efficacy of certain population groups, it may have the opposite effect on others depending on their appraisal of technology [71].

H6b: Machine agency affects computer self-efficacy.

3.7 Computer self-efficacy

As stated, self-efficacy is a personal belief in one's ability to achieve [16, 18]; and in terms of technology use, often referred to as computer self-efficacy, it may be understood as internal (a belief that I can do it myself) or external (a belief that I can do it with appropriate support) [19]. It is assumed that younger people are more willing to engage with technology and see what happens, which seems to be the case [22]. Further, since on the one hand people change in their experience and expectations, and on the other technology develops, so we need to be sensitive to such change especially in our metrics [20]. In HMN terms, it turns out that self-efficacy is related to trust and TAM constructs such as usefulness and ease-of-use [30]; and along with trust, it influences network behaviour [37]. Further, it is not self-esteem or extroversion which predict successful online presence, but self-efficacy [72]. Indeed, as well as social pressure (see Social Norms above), self-efficacy affects the willingness to engage in online networks [68]. We therefore hypothesise that:

H7a: Computer self-efficacy is positively correlated with the behaviour in HMNs.

On the other hand, it appears that self-efficacy is negatively correlated with anxiety [73], which may be associated with perceived risk [74]. So a second hypothesis obtains:

H7b: Computer self-efficacy is negatively correlated with perceived risk.

4   Research Design

Having established an initial research model and formulated a set of hypotheses (see **Table 1**, below) based on our review of pertinent literature over the past decade, we are now in the process of organising both qualitative and quantitative investigation of that model. Following a similar qualitative approach to [75], we are starting with a focus group of those familiar with trust as a concept, how it is traditionally thought to relate to human-to-human interactions, and how it may transfer to technology – our expert group – to provide an initial evaluation of our research model. We are targeting six to ten participants for this group. Using the feedback from that group to identify potential refinements, we will then conduct a quantitative survey using a set of questions based on the instruments suggested by researchers in our literature review [30, 31, 37, 48], but extended and updated to reflect experience in the specific environment of HMNs [20, 48]. In an attempt to avoid the demographic constraints in many studies where respondents are confined to undergraduate students or a similar cohort, we are creating a publically available survey to be hosted by the University of Southampton which will run for approximately four weeks. We will combine this with snowball participant sampling if necessary to achieve a target of some 200 valid responses. These will be analysed using a structural-equation modelling analysis in line with work reported in [48]. On this basis, we hope to be in a position to report our results and present a validated research model associated with our hypotheses in the coming months.

Table 1. Hypotheses

H1a	Perceived risk is negatively correlated with changes in regulation
H1b	Machine agency is negatively correlated with increasing levels of regulation
H1c	Regulation affects human agency
H2a	The perception of risk negatively affects trust in an HMN
H2b	The perception of risk negatively affects the behaviour in an HMN
H3a	HMN trust will positively influence the behaviour in an HMN
H3b	HMN trust will mediate human agency and the behaviour in an HMN
H4a	Social norms will affect the extent to which perceived risk influences behaviour in an HMN
H4b	Social norms will directly and positively correlate with behaviour in an HMN
H5a	Trust in the HMN is positively correlated with human agency
H5b	Human agency is related to self-efficacy
H6a	Machine agency in an HMN is directly related to human agency
H6b	Machine agency affects computer self-efficacy
H7a	Computer self-efficacy is positively correlated with the behaviour in HMNs
H7b	Computer self-efficacy is negatively correlated with perceived risk

5 Conclusions and Future Work

Based on a review of current work on computer self-efficacy, agency and trust, we have developed a model which extends work reported by Thatcher et al [31] to include a set of constructs known to influence these constructs and behaviour within online networks. Validating this model will increase our understanding of online behaviours which is of interest to those who engage with the networks, but also those who seek either to monitor and understand or regulate online behaviours, as well as those building networks who wish to explore factors which will support the long-term health of that network. More especially, our model seeks to extend our understanding of the interplay between agency and trust on the one hand, but also self-efficacy and indeed social influence on the other. What we have proposed is, therefore, intended to advance our general understanding of interactions between human and machine agency in human-machine networks. In this way, we hope to throw some light on how conscious as well as programmed agency influence one another and affect the willingness to engage online as well as individual self-belief in the capability to achieve personal goals.

References

1. Applin, S., Fischer, M.: Watching Me, Watching You.(Process surveillance and agency in the workplace). In: Technology and Society (ISTAS), 2013 IEEE International Symposium on. pp. 268–275. , Portland, OR (2013).

2. Tsvetkova, M., Yasseri, T., Meyer, E.T., Pickering, J.B., Engen, V., Walland, P., Lüders, M., Følstad, A., Bravos, G.: Understanding Human-Machine Networks: A Cross-Disciplinary Survey. arXiv Prepr. (2015).

3. Engen, V., Pickering, J.B., Walland, P.: Machine Agency in Human-Machine Networks; Impacts and Trust Implications. In: HCI International. Springer, Toronto, Canada (2016).

4. Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M.: The Socialbot Network: When Bots Socialize for Fame and Money. When Bots Social. Fame Money. 93 (2011).

5. Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S.: Who is Tweeting on Twitter: Human, Bot, or Cyborg? Proc. 26th Annu. Comput. Secur. Appl. Conf. - ACSAC '10. 21 (2010).

6. Rose, J., Jones, M.: The Double Dance of Agency: A Socio-Theoretic Account of How Machines and Humans Interact. Syst. Signs Actions. 1, 19–37 (2005).

7. Lee, J.D., Moray, N.: Trust, control strategies and allocation of function in human-machine systems. Ergonomics. 35, 1243–1270 (1992).

8. Norman, D.A.: Living with Complexity. MIT Press, Cambridge, MA (2010).

9. Berberian, B., Sarrazin, J.-C., Le Blaye, P., Haggard, P.: Automation technology and

sense of control: a window on human agency. PLoS One. 7, e34075 (2012).

10. Rose, J., Jones, M., Truex, D.: Socio-theoretic accounts of IS: The problem of agency. Scand. J. Inf. Syst. 17, 8 (2005).

11. Rose, J., Truex, D.: Machine Agency as Perceived Autonomy: An Action Perspective. In: Organizational and Social Perspectives on Information Technology. pp. 371–388. Springer (2000).

12. Applin, S., Fischer, M.: Cooperation between humans and robots: applied agency in autonomous processes'. In: 10th ACM/IEEE International Conference on Human/Robot Interaction, The Emerging Policy and Ethics of Human Robot Interaction workshop, Portland, OR (2015).

13. Jones, C., Healing, G.: Net generation students: agency and choice and the new technologies. J. Comput. Assist. Learn. 26, 344–356 (2010).

14. Jia, H., Wu, M., Jung, E., Shapiro, A., Sundar, S.S.: Balancing human agency and object agency: an end-user interview study of the internet of things. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. pp. 1185–1188. ACM Press, New York, New York, USA (2012).

15. Leonardi, P.M.: When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. MIS Q. 147–167 (2011).

16. Bandura, A.: Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. 84, 191 (1977).

17. Bandura, A.: Self-efficacy mechanism in human agency. Am. Psychol. 37, 122 (1982).

18. Bandura, A.: On the functional properties of perceived self-efficacy revisited. J. Manage. 38, 9–44 (2012).

19. Thatcher, J.B., Zimmer, J.C., Gundlach, M.J., McKnight, D.H.: Internal and external dimensions of computer self-efficacy: An empirical examination. Eng. Manag. IEEE Trans. 55, 628–644 (2008).

20. Marakas, G.M., Johnson, R.D., Clay, P.F.: The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. J. Assoc. Inf. Syst. 8, 15 (2007).

21. Mun, Y.Y., Hwang, Y.: Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. Int. J. Hum. Comput. Stud. 59, 431–449 (2003).

22. Simsek, A.: The Relationship between Computer Anxiety and Computer Self-Efficacy. Online Submiss. 2, 177–187 (2011).

23. Shu, Q., Tu, Q., Wang, K.: The impact of computer self-efficacy and technology dependence on computer-related technostress: A social cognitive theory perspective. Int. J. Hum. Comput. Interact. 27, 923–939 (2011).

24. Hildebrandt, M.: Profile Transparency by Design?: Re-Enabling Double Contingency. In: Hildebrandt, M. and de Vries, K. (eds.) Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology. pp. 221–246. Routledge, New York (2013).

25. Hildebrandt, M.: Promiscuous Data-Sharing in times of Data-driven Animism, (2016).

26. European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (2016).

27. Hildebrandt, M.: Smart Technologies and the End of Law: Novel Entanglements of Law and Technology. Edward Elgar Publishing Ltd, Cheltenham, UK (2015).

28. Featherman, M.S., Miyazaki, A.D., Sprott, D.E.: Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. J. Serv. Mark. 24, 219–229 (2010).

29. Poortinga, W., Pidgeon, N.F.: Exploring the dimensionality of trust in risk regulation. Risk Anal. 23, 961–972 (2003).

30. McKnight, D.H., Carter, M., Thatcher, J.B., Clay, P.F.: Trust in a specific technology. ACM Trans. Manag. Inf. Syst. 2, 1–25 (2011).

31. Thatcher, J.B., McKnight, D.H., Baker, E.W., Arsal, R.E., Roberts, N.H.: The Role of Trust in Postadoption IT Exploration: An Empirical Examination of Knowledge Management Systems. IEEE Trans. Eng. Manag. 58, 56–70 (2011).

32. Miltgen, C.L., Smith, H.J.: Exploring information privacy regulation, risks, trust, and behavior. Inf. Manag. 52, 741–759 (2015).

33. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Secur. Priv. 3, 26–33 (2005).

34. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science (80-.). 347, 509–514 (2015).

35. Lin, K.-Y., Lu, H.-P.: Why people use social networking sites: An empirical study integrating network externalities and motivation theory. Comput. Human Behav. 27, 1152–1161 (2011).

36. Kwon, O., Wen, Y.: An empirical study of the factors affecting social network service use. Comput. Human Behav. 26, 254–263 (2010).

37. Hsu, M.-H., Ju, T.L., Yen, C.-H., Chang, C.-M.: Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. Int. J. Hum. Comput. Stud. 65, 153–169 (2007).

38. Stewart, K.J.: Trust transfer on the world wide web. Organ. Sci. 14, 5–17 (2003).

39. McEvily, B., Perrone, V., Zaheer, A.: Trust as an organizing principle. Organ. Sci. 14, 91–103 (2003).

40. Bennett, S., Maton, K., Kervin, L.: The "digital natives" debate: A critical review of the evidence. Br. J. Educ. Technol. 39, 775–786 (2008).

41. Mayer, R.C., Davis, J.H., Schoorman, F.D.: AN INTEGRATIVE MODEL OF ORGANIZATIONAL TRUST. Acad. Manag. Rev. 20, 709–734 (1995).

42. Schoorman, F.D., Mayer, R.C., Davis, J.H.: An Integrative Model of Organizational Trust: Past, Present, and Future. Acad. Manag. Rev. 32, 344–354 (2007).

43. Beldad, A., de Jong, M., Steehouder, M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Comput. Human Behav. 26, 857–869 (2010).

44. Lewis, J.D., Weigert, A.J.: The Social Dynamics of Trust: Theoretical and Empirical Research, 1985-2012. Soc. Forces. 91, 25–31 (2012).

45. Chaouali, W., Yahia, I. Ben, Souiden, N.: The interplay of counter-conformity motivation, social influence, and trust in customers' intention to adopt Internet banking services: The case of an emerging country. J. Retail. Consum. Serv. 28, 209–218 (2016).

46. Sarker, S., Ahuja, M., Sarker, S., Kirkeby, S.: The role of communication and trust in global virtual teams: A social network perspective. J. Manag. Inf. Syst. 28, 273–310 (2011).

47. Friedman, B., Khan Jr, P.H., Howe, D.C.: Trust online. Commun. ACM. 43, 34–40 (2000).

48. Shin, D.-H.: The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interact. Comput. 22, 428–438 (2010).

49. Bandura, A.: Social Cognitive Theory: An Agentic Perspective. Annu. Rev. Psychol. 52, 1–26 (2001).

50. Fogg, B.: Persuasive computers: perspectives and research directions. In: The SIGCHI conference on Human Factors in Computing. pp. 225–232 (1998).

51. Garbarino, E., Strahilevitz, M.: Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. J. Bus. Res. 57, 768–775 (2004).

52. Kim, D.J., Ferrin, D.L., Rao, H.R.: A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decis. Support Syst. 44, 544–564 (2008).

53. Leventhal, H., Kelly, K., Leventhal, E.A.: Population Risk, Actual Risk, Perceived Risk, and Cancer Control: a Discussion. J. Natl. Cancer Inst. Monogr. 25, 81–85 (1999).

54. Covello, V.T.: Actual and Perceived Risk: A Review of the Literature. In: Technological Risk Assessment. pp. 225–245 (1984).

55. Brown, H.G., Poole, M.S., Rodgers, T.L.: Interpersonal traits, complementarity, and trust in virtual collaboration. J. Manag. Inf. 20, 115–137 (2004).

56. Tufekci, Z.: Can you see me now? Audience and disclosure regulation in online social network sites. Bull. Sci. Technol. Soc. 28, 20–36 (2008).

57. Strater, K., Lipford, H.R.: Strategies and struggles with privacy in an online social networking community. In: Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1. pp. 111–119. British Computer Society (2008).

58. Saravanakumar, C., Arun, C.: Survey on interoperability, security, trust, privacy standardization of cloud computing. In: 2014 International Conference on Contemporary Computing and Informatics (IC3I). pp. 977–982. IEEE (2014).

59. Følstad, A., Engen, V., Haugstveit, I.M., Pickering, J.B.: Automation in Human-Machine Networks: How Increasing Machine Agency Affects Human Agency. In: International Conference on Man-Machine Interactions [submitted] (2017).

60. Pavlou, P.A.: Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. 7, 101–134 (2003).

61. Giddens, A.: The Constitution of Society: Outline of the Theory of Structuration., (1984).

62. Li, X., Rong, G., Thatcher, J.B.: Does Technology Trust Substitute Interpersonal Trust? J. Organ. End User Comput. 24, 18–38 (2012).

63. Chow, W.S., Chan, L.S.: Social network, social trust and shared goals in organizational knowledge sharing. Inf. Manag. 45, 458–465 (2008).

64. Yee, N., Bailenson, J.N., Urbanek, M., Chang, F., Merget, D.: The unbearable likeness of being digital: The persistence of nonverbal social norms in online virtual environments. CyberPsychology Behav. 10, 115–121 (2007).

65. Lowry, P.B., Zhang, D., Zhou, L., Fu, X.: Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. Inf. Syst. J. 20, 297–315 (2010).

66. Cheung, C.M.K., Lee, M.K.O.: A theoretical model of intentional social action in online social networks. Decis. Support Syst. 49, 24–30 (2010).

67. Gefen, D., Straub, D.W.: Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. Omega. 32, 407–424 (2004).

68. Gangadharbatla, H.: Facebook Me. J. Interact. Advert. 8, 5–15 (2008).

69. Rose, J., Jones, M., Truex, D.: The Problem of Agency: How Humans Act, How Machines Act. In: International workshop on Action in Language, Organisations and Information Systems (ALOIS-2003) (2003).

70. Friedman, B., Kahn, P.H.: Human Agency and Responsible Computing: Implications for Computer System Design. J. Syst. Softw. 17, 7–14 (1992).

71. Gist, M.E., Mitchell, T.R.: Self-efficacy: A theoretical analysis of its determinants and malleability. Acad. Manag. Rev. 17, 183–211 (1992).

72. Krämer, N.C., Winter, S.: Impression Management 2.0. J. Media Psychol. 20, 106–116 (2008).

73. İskender, M., Akin, A.: Social self-efficacy, academic locus of control, and internet addiction. Comput. Educ. 54, 1101–1106 (2010).

74. Kim, Y.H., Kim, D.J., Hwang, Y.: Exploring online transaction self-efficacy in trust building in B2C e-commerce. J. Organ. End User Comput. 21, 37 (2009).

75. Dickinger, A., Arami, M., Meyer, D.: The role of perceived enjoyment and social norm in the adoption of technology with network externalities. Eur. J. Inf. Syst. 17, 4–11 (2008).