IFIPTM 2017 Graduate Symposium

Information Trust

Tosan Atele-Williams(✉) and Stephen Marsh

Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada
{tosan.atele-williams,stephen.marsh}@uoit.ca

Abstract. Information has been an essential element in the development of collaborative and cooperative models, from decision making to the attainment of varying goals, people are adept at making judgment on the trustworthiness of information, based on knowledge and understanding of a normative model of information. Contemporary narrative especially in high-impact contexts like politics, health, business, government and technology, is eroding trust in information, its source, its value and the ability to objectively determine the trustworthiness of a piece of information, a situation made more complex by social networks, social media have made the spread of information easier and faster irrespective of their trustworthiness, hence the need for judgment on the trustworthiness of a piece of information based on social cognitive construct, a trust model for information.

Keywords: Computational trust · Information trustworthiness · Decision support · Trust properties · Information value

1 Introduction

Various information behavior models, suggest a normative model of information as true, complete, valid, can be relied on as being correct and from a trusted source [1]; census data from statistics Canada can be regarded as valid and from a trusted source which can be reliably used for planning purposes, and as an economic tool, such data should carry more trusted weight than information sourced from a third party sources or social media platforms. Other normative information behavior prescribes trusted information as timely in the sense that it should be from a precise time period [1, 2], for example when analyzing census data for planning and developmental purposes it is paramount to look at current or the most recent figures. Information is of no value or worth the investment of time and money, especially in making business decisions if it is not relevant, does not have the right amount of details, cannot be easily stored in a way that it can be accessed effortlessly, or easily understood by the end user [1, 2, 4]. Other factors that add value and trustworthiness to information include but not limited to its accuracy, consistency, and completeness. Despite the best effort of information scientist on the nature of information, and work on information literacy behavior misinformation and disinformation still permeates social networks [1, 4], social media platforms like twitter and Facebook has helped in the spread of inaccurate information, a culture emboldened by need to share information even when the validity of the information

J.-P. Steghöfer and B. Esfandiari (Eds.): IFIPTM 2017, IFIP AICT 505, pp. 221–222, 2017.
DOI: 10.1007/978-3-319-59171-1

cannot be vouched for or when the person sharing such information does not believe it but regardless still goes ahead to share because it serves a narrative, a means to manipulate rather than to inform, as a source of social influence [3], as demonstrated by the recent political and business climate in the west that have added relatively new lexicons like fake news and alternate facts.

The consequences of deceptive and misleading information can be far-reaching for governments, citizens, business institutions, data professionals, and designers, it can create an atmosphere of mistrust, distrust, confusion, panic, and it can influence decisions and damage reputations. Information agents, brokers may find it difficult to use information, or seek alternate and less reliable sources of information because of the air of uncertainty, hence the need for an information model based on computational trust [5, 7], a paradigm drawn from a social, cultural, historical and psychological context and much more aspects of relationships [6], trying to model the best in these related milieus computationally.

Trust as a computational concept is important in understanding the thought process with regard to choice, options and decision-making process in human and computer interactions, especially in situations where there is a measure of risk [7, 8]. The goal is to formulate a theoretical framework; a socio-cognitive construct for the trustworthiness of information based on cues of credibility and deception, a model to assist judgment calls and an expectation of when, trust and its fulfillment can be expected.

Information does not exist in a vacuum, how it is perceived and used is influenced by a number of social, cultural, and historical factors, hence the need for an inclusive and context-aware information literacy behavior [1], our goal is to incorporate the characteristics of information; reliability, validity, and importance into a trust model, depending on the context, the model will also factor in the reputation of a source, the value of the information and cues to credibility and deception, with the aim of enabling agents to make judgments and situational decisions about the trustworthiness of information.

References

1. Karlova, N.A., Fisher, K.E.: A social diffusion model of misinformation and disinformation for understanding human information behavior. Inf. Res. **18**(1), 1–17 (2013)
2. Craig, S.: Lies, damn lies, and viral content. How news websites spread (and debunk) online rumors, unverified claims, and misinformation. Tow Center for Digital Journalism (2015)
3. Barber, K.S., Kim, J.: Belief revision process based on trust: agents evaluating reputation of information sources. In: Falcone, R., Singh, M., Tan, Y.H. (eds.) Trust in Cyber-Societies. LNCS, vol. 2246, pp. 73–82. Springer, Heidelberg (2001)
4. Marsh, S.: infoDNA (Version 2) Agent Enhanced Trustworthy Distributed Information. PST (2004)
5. Witkowski, M., Artikis, A., Pitt, J.: Experiments in building experiential trust in a society of objective-trust based agents. In: Falcone, R., Singh, M., Tan, Y.H. (eds.) Trust in Cyber-Societies. LNCS. vol, 2246, pp. 111–132. Springer, Heidelberg (2001)
6. Piotr, S.: Trust: A Sociological Theory. Cambridge University Press (1999)
7. Marsh, S., Briggs, P.: Examining trust, forgiveness and regret as computational concepts. Computing with Social Trust, pp. 9–43. Springer London (2009)
8. Golbeck, J. (ed.): Computing with Social Trust. Springer Science Business Media (2008)

Privacy and Trust in Cloud-Based Marketplaces for AI and Data Resources

Vida Ahmadi Mehri(✉) and Kurt Tutschku

Blekinge Institute of Technology, Karlskrona, Sweden
{vida.ahmadi.mehri,kurt.tutschku}@bth.se

Abstract. The processing of the huge amounts of information from the Internet of Things (IoT) has become challenging. Artificial Intelligence (AI) techniques have been developed to handle this task efficiently. However, they require annotated data sets for training, while manual preprocessing of the data sets is costly. The H2020 project "Bonseyes" has suggested a "Market Place for AI", where the stakeholders can engage trustfully in business around AI resources and data sets. The MP permits trading of resources that have high privacy requirements (e.g. data sets containing patient medical information) as well as ones with low requirements (e.g. fuel consumption of cars) for the sake of its generality. In this abstract we review trust and privacy definitions and provide a first requirement analysis for them with regards to Cloud-based Market Places (CMPs). The comparison of definitions and requirements allows for the identification of the research gap that will be addressed by the main authors PhD project.

Keywords: Privacy · Trust · Marketplace · IoT · Cloud · AI

1 A Market Place for Artificial Intelligence and Data

Bonseyes' Market Place (MP) for AI [1–4] aims at engaging the various stakeholders, e.g. data providers, model, or application designer, into business among AI resources, i.e. data sets, models, training facilities, etc. The business around the resources may accelerate the model design and reduces the design costs. The MP will provide functions to offer, sell, pay or use AI resources and data sets. The proposed MP will be implemented by a cloud system in order to deal with the large size of data sets and to permit elasticity for the AI resources. This led to the notion of a CMP. As any MP, a CMP requires mechanisms to enforce *privacy* and *trust*. However, the separation between resource location (e.g., storage location) and resource availability (e.g. data availability) in cloud systems makes it more challenging to implement trustful mechanisms for these features as in non-virtualised systems.

J.-P. Steghöfer and B. Esfandiari (Eds.): IFIPTM 2017, IFIP AICT 505, pp. 223–225, 2017.
DOI: 10.1007/978-3-319-59171-1

2 Trust and Privacy Definitions for Network and Clouds

Trust and Trust Dimensions: a widely agreed definition for *trust* in networks, Clouds and systems is given in IETF Internet security glossary: as "... the extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions" [5]. The view of applications, Clouds and networks as "systems" leads to the definition of multiple *trust dimensions* [6]. These dimensions comprise (a) "device trust", i.e. the reliability of IoT devices to produce data correctly, (b) "operation trust", refers to the combination of data traceability and analytics, (c) "communication trust", builds on confidentiality, integrity, and authenticity in data transmission, (d) "infrastructure trust", which aims at the transparency and predictability of processing.

Privacy and Privacy Dimensions: the IETF glossary also provides a definition for *privacy*: "... the right of an entity to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others" [5]. R.S. Poore defines privacy as a required context of personal Identifiable Information (PII) which have to be under control of the individual person who is the owner of it [7].This view on privacy leads to *privacy dimensions* such as, cf. [6, 8]:

- Identity privacy: avoid the disclosure of users identity
- Location privacy: avoid the disclosure location information for specific user
- Device privacy: avoid the disclosure of device and security information
- Communication privacy: refers to encryption algorithm for confidentiality
- Access privacy: privilege levels for authorised data access
- Operation privacy: avoid the disclosure of data processing techniques
- Footprint privacy: avoid the identity disclosure by behavioural analysis
- Query privacy: avoid the identity disclosure by analysis of the origin of queries

3 Privacy and Trust Requirements for CMPs

In general, the privacy levels for an AI resource or a data set depend on the importance of the resource or of the type of PII stored in it. For example, medical records need very high levels of protection since a leakage of information may embarrass a specific person. Hence, if such data sets are traded then the specific levels of privacy needs to be maintained at the various locations where the data is accessed or processed, otherwise the users will lose their *trust* into the MP.

CMPs might host data sets with very different privacy levels at very different locations. As a result, they must enable a differentiated, transparent and even traceable handling of data. Some data sets may not be allowed to leave a certain physical premise due to regulation or provider policy, while others can do so. A CMP must support both modes of data availability at the required privacy levels for the sake of its generality. This feature is often denoted as the ability for "privacy by design" [9] of an architecture.

Since data sets are associated in a MP with a value, the infringement of this value by disclosing the data to other users needs to be avoided. Here, the privacy requirements, as seen from the data provider, turn into the problem of "Digital Right Management" that needs to be addressed by the MP architecture or its mechanisms and functions.

4 Conclusion

It is obvious that the definitions of trust and privacy do not directly address the virtualisation features of Cloud system. Particularly, the implications by separating between storage location and data availability in the Cloud are not clear yet. The privacy and trust dimensions might partly match with the application requirements of CMPs. Hence, their suitability for evaluation Cloud mechanisms needs to be investigated. These investigations as well as the design of mechanism for privacy and trust in CMPs will define the work in this PhD project.

Acknowledgment. This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 732204 (Bonseyes). This work is supported by the Swiss State Secretariat for Education Research and Innovation (SERI) under contract number 16.0159. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

References

1. BONSEYES - Artificial Intelligence Marketplace. https://www.bonseyes.com/
2. Bonseyes Consortium. Grant agreement number - 732204 bonseyes - annex 1 (part a): Description of action. Available on request from Bonseyes Consortium at https://www.bonseyes.com/, October 2016
3. Fricker, S., Maksimov, Y.: Pricing of data products in data marketplaces. In: 8th International Conference on Software Business (ICSOB) (2017, in submitted)
4. Llewellynn, T., Milagro, M., Deniz, O., Fricker, S., Storkey, A., Pazos, N., Velikic, G., Dahyot, R., Koller, S., Goumas, G., Leitner, P., Dasika, G., Wang, L.: Bonseyes: platform for open development of systems of artificial intelligence. In: ACM International Conference on Computing Frontiers (2017, in submitted)
5. RFC 2828. Internet security glossary, May 2000
6. Daubert, J., Wiesmaier, A., Kikiras, P.: A view on privacy and trust in iot. In: 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 2665–2670, June 2015
7. Poore, R.S.: Anonymity, Privacy, and Trust. Inf. Syst. Secur. **8**(3), 16–20 (1999)
8. Cheng, Y., Naslund, M., Selander, G., Fogelström, E.: Privacy in machine-to-machine communications a state-of-the-art survey. In: 2012 IEEE International Conference on Communication Systems (ICCS), pp. 75–79, November 2012
9. Article 29 data protection working party and working party on police and justice, the future of privacy. Joint contribution to the Consultation of European Commission on the legal framework for the fundamental right to protection of personal data, WP168, December 2009

Psychological Evaluation of Human Choice Behavior in Socio-Technical Systems: A Rational Process Model Approach

Tim Schürmann(✉)

Technische Universität Darmstadt, Darmstadt, Germany
schuermann@psychologie.tu-darmstadt.de

In the age of digital services and everyday smartphone usage, the issue of online privacy has gathered more and more interest for researchers, service providers and consumers. Assuming one's digital information is private is equivalent to trusting service providers to handle one's data in a certain way or ensuring protective measures against loss of privacy. When a consumer registers for an online service or installs a smartphone app, I assume an internal psychological process to relate the benefits of their decision to the risks associated with it. However, this process is considered to be subject of uncertainty. Therefore, decisions in a socio-technical environment can be viewed as decisions governed by a probabilistic amount of trust in an outcome, or, in other words, the amount of belief one holds that a hypothesis about future events will turn out to be true.

Previous research on human online behavior paints a fairly bleak picture of how we handle said uncertainty. It often adopts the paradigm of the Homo Heuristicus [1], relying on computational shortcuts rather than normatively rational inference. In a scenario as complex as online privacy, it also points out how unlikely it is for users to have a complete understanding of the capabilities and motives of involved parties [2].

However, psychological research on broader decision making processes includes evidence that humans are in fact able to combine information in a rational sense [3]. The Sampling Hypothesis [4] may provide the grounds for unifying research on heuristic or otherwise boundedly rational decision making on one hand with a rational account on the other. It does so by approximating Bayesian inference, sampling from probability distributions over possible hypotheses or parameter values instead of using these full distributions and creating implausibly complex computations. Its application shows that specific effects like the availability heuristic can actually be considered by-products of its sampling process [5]. Vul [4] provides evidence that in many situations, sampling only a very limited number of times provides a computationally similar result to using full yet analytically intractable probability distributions. Specifically, he links the benefits of sampling to the consumption of energy and time while arriving at a decision: why make one time- and energy-consuming decision perfectly maximizing my chance of success, when I can make many "good enough" decisions that approximate optimal results in the long run? This globally optimal solution however can produce seemingly irrational local behavior. Models that utilize such approximate Bayesian inference are termed rational process models [6].

J.-P. Steghöfer and B. Esfandiari (Eds.): IFIPTM 2017, IFIP AICT 505, pp. 226–228, 2017.
DOI: 10.1007/978-3-319-59171-1

It appears as though human subjects, while certainly limited in their cognitive resources and computational capabilities as laid out by the bounded rationality paradigm, may make use of this process: they operate by maximizing success chances and making rational choices, but on a global rather than local level. My work utilizes this type of model to investigate how humans make decisions online, and more importantly how to sensitize them to make more adequate decisions to protect their private information. A preliminary study [7] indicates that answers to these questions are not as simple as pointing to a specific heuristic approach or a systematic gap between privacy-related attitudes and behavior. When asked whether they wanted to install a travel-related smartphone app involving beneficial and non-beneficial features, subjects showed behavioral patterns that were predicted by a rational process model. Preference trade-offs for the app's features form the basis of the model prediction as a posterior distribution. Then, sampling from said individual posterior provides the model with an approximate probability of choosing to install the app. The model stochastically chooses the option with higher utility according to its probability. It therefore allows for a seemingly irrational decision on the local level when choosing the option with lower utility instead. The rate with which subjects chose their higher utility option or deviated from it was predicted by the model, with a deviation of approximately 5% between its prediction and the empirical data. This deviation is not significantly different from zero, as indicated by a Bayesian estimation of the difference parameter between the two.

The model seems to capture the process with which subjects combine preferences about features as well as their trade-off between utility maximization and cognitive resource management. It is based on subjective utility distributions, thus avoiding the assumption of complete situational knowledge proposed in previous research [2] to arrive at a rational decision. These subjective utility distributions in turn can be learned solely based on past experience [8]. It is worth noting that heuristic or probability-weighted alternatives of the model, following a cumulative prospect theory (CPT) approach, could possibly have resulted in a decent statistical fit as well. CPT's parameter estimation [9] would likely capture stochastic variations descriptively if it was retrospectively fitted for a specific individual and trial. It would not, however, explain the nature of the variation or the necessity of the sampling process on theoretical grounds. Meanwhile, the rational process model approach outlined here unites the idea of Bayesian computational rationality in human cognition with limitations on the algorithmic level [10]. Additionally, it allows for an explanation of other phenomena observed in decision making research, like probability matching.

Based on the preliminary study, I plan to first adapt the model to other interactions with socio-technical systems. Secondly, I will explore specific mechanisms of the model to apply them to privacy interventions. For example, increasing the number of samples drawn in the model increases the chance of choosing an option with higher utility, instead of sometimes choosing a lower utility option. This may be achieved by asking subjects to state their choice repeatedly. Assuming a privacy-protecting decision (not installing an app that requires permissions to access private data) is a subject's higher utility option, an intervention increasing their internal sample count should result in a higher probability of choosing that option. However, there is a chance that they favor a privacy-disclosing option. In that case, an intervention designed to increase sampling counts might reinforce the tendency to pick the disclosing option, resulting in

the opposite of the intended purpose. Future work will draw inspiration from how the mechanisms of sampling in decision making work to design privacy-protecting interventions tailored to individual preferences and thereby making use of the human tendency to operate on a globally rational level of information integration. Building on these rational process mechanisms, I aim to assess and direct user trust in the interaction with socio-technical systems as well as explain stochastic deviance from their expected behavior.

References

1. Gigerenzer, G., Brighton, H.: Homo heuristicus: why biased minds make better inferences. Top. Cogn. Sci. **1**, 107–143 (2009). doi:10.1111/j.1756-8765.2008.01006.x
2. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Secur. Priv. Mag. **3**(1), 26–33 (2005). doi:10.1109/MSP.2005.22
3. Griffiths, T.L., Tenenbaum, J.B.: Optimal predictions in everyday cognition. Psychol. Sci. **17** (9), 767–773 (2006). doi:10.1111/j.1467-9280.2006.01780.x
4. Vul, E., Goodman, N., Griffiths, T.L., Tenenbaum, J.B.: One and done? Optimal decisions from very few samples. Cogn. Sci. **38**(4), 599–637 (2014). doi:10.1111/cogs.12101
5. Sanborn, A.N., Chater, N.: Bayesian brains without probabilities. Trends Cogn. Sci. **20**(12), 883–893 (2016). doi:10.1016/j.tics.2016.10.003
6. Sanborn, A.N., Griffiths, T.L., Navarro, D.J.: Rational approximations to rational models: alternative algorithms for category learning. Psychol. Rev. **117**(4), 1144–1167 (2010). doi:10.1037/a0020511
7. Schürmann, T., Smirny, J., Zimmermann, S., Vogt, J.: Adoption behavior of smartphone apps gathering private data is explained by a sampling-based rational process model. Manuscript in preparation (2017)
8. Srivastava, N., Schrater, P.: Learning what to want: context-sensitive preference learning. PLoS ONE **10**(10), e0141129 (2015). doi:10.1371/journal.pone.0141129
9. Boos, M., Seer, C., Lange, F., Kopp, B.: Probabilistic inference: task dependency and individual differences of probability weighting revealed by hierarchical bayesian modeling. Front. Psychol. **7**, 755 (2016). doi:10.3389/fpsyg.2016.00755
10. Marr, D.: Vision: A Computational Investigation into the Human Representation and Processing of Visual Information. The MIT Press (2010). doi:10.7551/mitpress/9780262514620.001.0001

Author Index