

Trust and Distrust in e-Democracy

David Duenas-Cid
Gdańsk University of Technology
david.duenas.cid@pg.edu.pl

Tomasz Janowski
Gdańsk University of Technology and
Danube University Krems
tomasz.janowski@pg.edu.pl

Robert Krimmer
University of Tartu
robert.krimmer@ut.ee

ABSTRACT

In the digital government research literature, the concept of trust is typically used as a precondition for the adoption of digital technology in the public sector or an outcome of a roadmap leading up to such adoption. The concept plays a central role in many decisions linked to the planning, adoption and management of the public sector technology. In contrast, the concept of distrust is almost neglected in such literature but, when approached, it appears as the opposite logical side of the trust-distrust dichotomy. However, we conjecture that the path to building trust is different than the path to building distrust and both concepts should be regarded as different theoretical constructs. The workshop aims to prove this conjecture drawing on the insights from the field of e-democracy including internet voting. Given its technical breadth, political and societal implications, and layers of complexity, e-democracy is a good benchmark for exploring this topic. The workshop will confront the main conjecture using examples, research and experiences contributed by participants, conceptual and methodological tools introduced by the organizers, and a discussion shared by everybody. The outcome – elements that help build trust or distrust in various forms of e-democracy – will have practical and theoretical implications, aiming at further research by the participants and collective publication of the results in a special issue in a top ranked journal, preferably Government Information Quarterly.

CCS CONCEPTS

• Applied Computing; • Security and Privacy; • Human Centered Computing;

KEYWORDS

Trust, Distrust, e-Democracy, Internet Voting, Privacy, Security, Perception

ACM Reference Format:

David Duenas-Cid, Tomasz Janowski, and Robert Krimmer. 2022. Trust and Distrust in e-Democracy. In *DG.O 2022: The 23rd Annual International Conference on Digital Government Research (dg.o 2022), June 15–17, 2022, Virtual Event, Republic of Korea*. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3543434.3543637>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

dg.o 2022, June 15–17, 2022, Virtual Event, Republic of Korea

© 2022 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-9749-0/22/06.

<https://doi.org/10.1145/3543434.3543637>

1 INTRODUCTION

The concept of trust is a foundation for the functioning of the democracy. The depersonalization of the social life demands trust-building with individuals and institutions to secure social order and handle complexity [10, 14]. The use of technology for government purposes, while searching for more convenient ways of interacting with citizens, brings along a new set of complexities and challenges [6]. e-Democracy follows a similar trend, aimed at keeping citizens engaged in decision-making processes [1, 16] by interacting with convenient and efficient systems [7], but also facing challenges that make implementation [9] and adoption [15] difficult. One of such challenges is assuring trust.

Following Luhmann [10], we understand trust as the bridge that connects the known with the unknown and allows taking decisions that might entail risks; in other words, it is a mechanism of dealing with complexity and uncertainty. When putting this definition to work with e-Democracy, the relevance of collective decision making and power delegation, and the complexing of the technological environment involved, make the comprehension of the working of trust more relevant than ever. Although several efforts have been undertaken to understand trust, this concept is often regarded as a logical outcome of the presence of a set of factors such as, e.g. transparency [3], usability [2], security [13] and verifiability [8]. In contrast, the concept of distrust is generally left out of the analysis or, when considered, placed at the opposite end of the trust-distrust dichotomy [4]. A negative outcome that should be actively avoided in order to ensure the success of technology [5], despite its usefulness for detecting problems [11] or vulnerabilities [12] in implemented systems.

The key premise of this workshop is tackling the separate nature of trust and distrust in the field of e-Democracy. While related, the concepts are separate theoretical constructs and should be subject to separate analysis. In other words, the paths that bring about the creation of trust and distrust co-exist but are different: the opposite to “trust” is “not to trust” and not “distrust”, while the opposite of “distrust” is “not to distrust” and not “trust”. This distinction makes possible understanding which arguments contribute to the creation of trust, distrust or both, and how they contribute. An example is a voting system which technical robustness is contributing to the creation of trust due to increased safety but also distrust due to the general population not understanding the complex working of such systems [13]. Thus both paths should be approached separately but allowing individuals or institutions to negotiate their positions on the trust-distrust dichotomy on the use of technology in democracy and how such use influences the collective outcome, i.e. the quality of the democracy itself.

While studying the trust-distrust dichotomy is relevant to various fields of Digital Government, we chose e-Democracy for two

main reasons. The first is the need to better understand the functioning of our democracies, particularly when the use of technology changes the democratic rules of the game. The second is that e-Democracy projects, due to their diversity, allow collecting different perspectives on the topic, from specific contexts where local dynamics of social interactions serve as good explanatory elements, to the use of internet voting systems in elections. This diversity affects the comprehension of the elements that might help understand the creation of trust and distrust. Not the same elements are relevant when we are talking about social participation, which is diverse, localized and less demanding on technical requirements and time constraints, than when we approach the electoral field, which is more standardized internationally, imposes strict time constraints and requires high levels of security, privacy and integrity.

2 GOAL AND OBJECTIVES

The workshop will be organized under the umbrella of the ELECTRUST project “Dynamics of Trust and Distrust Creation in Internet Voting” funded by the European Commission’s Horizon 2020 program over the 2022-2023 period. The workshop will contribute to the project goals by debating the notions of trust and distrust in the field of e-Democracy by inviting experts in the field who can share their expertise in the use of technology for democratic purposes. The organizers will introduce conceptual and methodological tools to study trust and distrust in e-Democracy, the tools will be applied to the examples, research and experiences contributed by experts, leading to the creation of trust or distrust in e-Democracy, and the workshop will be concluded by discussion and synthesis of findings. The workshop results will contribute to the creation of a common ground of knowledge to be shared amongst the participants and to be continued in further venues. The expected outcomes will be of interest to researchers but also to practitioners and decision-makers. They will also contribute to the development of the theoretical framework of the ELECTRUST project, and will lead to the creation of a network of participants and to potential common publications. In particular, the organizers will aim at developing a special issue of *Government Information Quarterly*.

3 WORKSHOP STRUCTURE AND PARTICIPANT PROFILES

The workshop is expected to cover a wide range of experiences in the field of e-Democracy. The profiles should be selected amongst participants who can unfold their knowledge by providing an analysis of cases where the trust-distrust dimensions might be relevant: implementation of new projects, analysis of successful or failed experiences, theoretical analysis of elements bringing trust or distrust, etc. Given the diverse nature of e-Democracy, the participants will not be restricted to one single type of contribution. The conditions for the implementation of technological solutions to transform social participation systems are very different than when such solutions are proposed for elections. The different realities will enrich the comprehension of the elements affecting each of them.

- Welcome participants and self-introduction – 15 mins
- Electrust Project introduction – 15 mins
- Contributions from participants – 30 mins
- Open Discussion – 20 mins

- Conclusions – 10 mins

For the discussion, and using the presented cases as a benchmark to relate to, the workshop will pose questions including but not limited to the following:

- How does the creation of trust or distrust affect democracy and e-Democracy?
- How is the technological transformation of democracy and public administration contributing to the creation of trust or distrust?
- What actors are involved in the creation of trust or distrust? How is the use of technology changing them?
- How is trust and distrust distributed amongst technology users?
- How to assess the impact of a given technology on the creation of trust or distrust? Which indicators can be used?
- What are the most successful or unsuccessful elements for the creation of trust?
- How would they work in a different technological, institutional or cultural context?

ACKNOWLEDGMENTS

The project ELECTRUST has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101038055

REFERENCES

- [1] Alvarez, R.M., Hall, T.E.: *Point, click, and vote: The future of internet voting*. Brookings Institution Press, Washington DC (2004).
- [2] Carter, L., Campbell, R.L.: Internet voting usefulness: An empirical analysis of trust, convenience and accessibility. *Journal of Organizational and End User Computing*. 24, 3, 1–17 (2012). <https://doi.org/10.4018/joec.2012070101>.
- [3] Gjøsteen, K.: Analysis of an internet voting protocol. *IACR Cryptology ePrint Archive*. 1–16 (2010). https://doi.org/10.1007/978-3-642-32747-6_1.
- [4] Hopland, L., Hole, K.: Building and Maintaining Trust in Internet Voting. *Computer*. 74–80 (2012). <https://doi.org/10.4018/9781930708198.ch005>.
- [5] IDEA - International Institute for Democracy and Electoral Assistance: *Introducing Electronic Voting: Essential Considerations*. International IDEA (2011).
- [6] Janowski, T.: Digital government evolution: From transformation to contextualization. *Government Information Quarterly*. 32, 3, 221–236 (2015). <https://doi.org/10.1016/j.giq.2015.07.001>.
- [7] Krimmer, R. et al.: New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? *Public Money and Management*. 41, 1, 17–26 (2021). <https://doi.org/10.1080/09540962.2020.1732027>.
- [8] Kulyk, O., Volkamer, M.: Usability is not Enough: Lessons Learned from ‘Human Factors in Security’ Research for Verifiability. In: Krimmer, R. and Volkamer, M. (eds.) *Third International Joint Conference on Electronic Voting (E-Vote-ID 2018)*. pp. 66–81 TUT Press, Bregenz (2018).
- [9] Licht, N. et al.: To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In: Krimmer, R. et al. (eds.) *Electronic Voting, E-Vote-ID 2021. Lecture Notes in Computer Science*. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-86942-7_7.
- [10] Luhmann, N.: *Trust and Power*. Wiley-Blackwell, Chichester (1979).
- [11] McKnight, H., Chervany, N.: Trust and Distrust Definitions: One Bite at a Time. In: Falcone, R. et al. (eds.) *Trust in Cyber-societies Integrating the Human and Artificial Perspectives*. pp. 27–55 Springer-Verlag, Berlin (2001).
- [12] Oostveen, A.-M.: Outsourcing Democracy: Losing Control of e-Voting in the Netherlands. *Policy & Internet*. 2, 4, 201–220 (2010). <https://doi.org/10.2202/1944-2866.1065>.
- [13] Oostveen, A.-M., van den Besselaar, P.: Security as belief User’s perceptions on the security of electronic voting systems. *Electronic Voting in Europe: Technology, Law, Politics and Society*. 47, May 2014, 73–82 (2004).
- [14] Simmel, G.: The sociology of secrecy and of secret societies. *The American Journal of Sociology*. XI, 11, 441–498 (1906).
- [15] Toots, M. et al.: Success in evoting - Success in e-Democracy? The Estonian paradox. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. pp. 55–66 (2016). https://doi.org/10.1007/978-3-319-45074-2_5.



- [16] Vayenas, C.: Democracy in the Digital Age. How we'll vote and what we'll vote about. Arena Books, Bury Saint Edmunds (2017).