UvA-DARE (Digital Academic Repository)

The commodification of trust

Bodó, B.

Publication date
2021

Document Version
Final published version

License
CC BY-NC-ND

[Link to publication](#)

The commodification of trust

blogs.lse.ac.uk/businessreview/2021/06/21/the-commodification-of-trust/

June 21, 2021

The internet and digital technologies created a new category of trust producers. Online reputation management services (such as Uber or Airbnb), distributed ledgers, and AI-based predictive systems offer familiarity, control, and insurance by structuring social, economic interactions via technical systems. **Balázs Bodó** *writes that even though these infrastructures are widely used within public and private institutions, we have no reason to trust them. He argues that we must increase the trustworthiness of technological trust infrastructures — and stop using them if that is not possible — lest commodified forms of trust endanger the social and economic relations that they mediate.*

The ongoing COVID crisis has brought to the forefront the complex trust relationships between citizens, public and private institutions, and various digital technologies. Can I trust a face mask to protect me from infection? Should I trust the person (not) wearing a mask? Should I trust the pandemic-related advice of governments and scientists? Can we, as a society, trust the brand-new mRNA vaccine technology? Is a traditional vaccine technology more or less trustworthy, if it is coming from an authoritarian regime such as Russia and China? Can I trust my government or the European specialised agencies (such as the European Medicines Agency) to correctly assess the health risks associated with different vaccine technologies, and not succumb to economic or political pressures?

Can the government trust its citizens to voluntarily follow non-mandatory quarantine advice? Can a government be trusted with running contact tracing and vaccination passport schemes? Do employers trust their workforce to work from home, or do they prescribe the use of monitoring technologies? Can we trust our teleconferencing infrastructure, so they work reliably, and protect our privacy? Can we have confidence in the third-party teaching materials and e-learning environments that schools are now forced to use to teach and assess our children? And, as the case of the UK government's debacle with their grading AI suggests, when these systems are misfiring, how does that affect trust in the government?

Trust is the strategy humans employ to cross the bridge of uncertainty in their social, economic relations, so they can live with, rely on, or cooperate with each other in the face of risks, contingencies, and potential harm.

Trust as a course of action may be specific to each individual and trust relationship, but trust relies on a number of common precursors, which may facilitate or hinder its emergence:

familiarity, control, and insurance (Sztompka, 1998; Zucker, 1985). Familiarity refers to situational normalcy, shared background expectations, predictability, epistemic certainty. A sense of control may be provided by the ability to agree on clear rules (via, for example contracts or laws), transparency, accountability, oversight, and enforcement. Insurance means the ability to mitigate risks and reduce potential harms that all trusting relationships naturally entail.

When we have to make a trust decision, we have multiple trust facilitating infrastructures to turn to for familiarity, control, and insurance. People can listen to the public service broadcaster, scientists, or online gossip networks for information on vaccines and masks. Governments can use AI systems or the mix of human judgement and administrative rules to make decisions of welfare fraud, policing or grading in education. People can turn to friends, systems like Uber or Airbnb, or big brand hospitality companies for transportation or hospitality.

Our societies have developed three kinds of trust infrastructures over time: communal, private, and public. **Communal trust** infrastructures constitute the most ancient and pervasive forms of trust production. Familiar, ethnic, religious, or tribal relations, professional associations, epistemic or value communities, groups with shared location or shared past are the most reliable sources of familiarity, control, insurance.

Public trust infrastructures produce trust as a public good. In modern societies we have long been depending on abstract, institutionalised frameworks, whose aim is to produce trust in a society of strangers. Public institutions such as public education, public service media; fair, transparent, accountable, disinterested public administration; the legislative, judicial, and law-enforcement bodies of the state, as well as societal institutions, such as the press, or science create familiarity, control, and insurance in social, political, and economic relations.

Lastly, **private trust infrastructures** produce and offer trust as a commodity on the marketplace. Lawyers, accountants, credit rating agencies, insurers, but also banks, commercial brands, or the Mafia offer trust for a fee. In all these cases trust is sold as a service to clients who pay for the reduction of complexity and some form of certainty or control, while the trust producer captures some of the value created in the trust-facilitated economic transactions.

The internet and digital technologies created a new category of trust producers. Online reputation management services, distributed ledgers, and AI-based predictive systems offer familiarity, control, and insurance by structuring social, economic interactions via technical systems. Reputation management services, such as Uber or Airbnb provide some form of familiarity through their **control of our relationship to the past**. Search engines, social media, and e-commerce platforms preserve traces of past actions, statements, information, which we, as hopeful trustors then use to establish the identity, reputation, character of

individuals and institutions we consider trusting. Other technical systems try to produce trust through extending their **control over the present**. Digital Rights Management systems, blockchains, and other smart contract based technical systems create restrictive and prescriptive technical environments in which one can be confident in the expected behaviour and performance of the other. Lastly, machine learning algorithms produce **trust by reducing future uncertainty**, creating predictability, and offering tools to manage risks. AI, automated decision-making, and predictive systems reduce complexity, the number of future alternatives, and create a fictious, but nevertheless effective elimination of future contingencies in order to sustain the illusion of a navigable, and manageable present.

These technical trust infrastructures pose a number of serious challenges. They are widely used within public and private institutions, and in almost every social, economic, political, cultural relation between citizens, citizens and governments, citizens and businesses, businesses and businesses. Yet, their trustworthiness is dubious: as I argue elsewhere, we have few opportunities to establish their trustworthiness, and no reason to trust them. Their prominence also upsets (disrupts, in their parlance) the role other trust infrastructures play in our relations. If a government AI system fails, the trust in the public trust infrastructure takes a hit. If there is a growing distrust in government, often highly ideological and political, communal and tribal trust networks take up the task of providing epistemic certainty, and familiarity – which may easily lead to the rapid fragmentation of society. At the other end of the spectrum (and the globe), public and private technological infrastructures can merge into a dystopian order, as many fear to be the case with the Chinese social credit system. Not having access to private trust infrastructures may have devastating consequences as platform workers who lost their accounts and reputation scores, and the deplatformed Donald Trump have learned the hard way.

The current crises around trust also spell out the tasks ahead. We have to increase the trustworthiness of technological trust infrastructures and stop using them if that is not possible. We have to preserve and increase trust in our public trust infrastructures. And most importantly, we have to make sure that the private, commodified form of trust do not endanger all those social, economic relations which they enter.

♣♣♣

Notes:

- *This blog post is based on The Commodification of Trust (May 11, 2021). Blockchain & Society Policy Research Lab Research Nodes 2021/1. Additional literature: Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators, New Media & Society; and Here be dragons – maintaining trust in the public sector in face of emerging tech (June 16, 2021).*

- *The post expresses the views of its author(s), and do not necessarily represent those of LSE Business Review or the London School of Economics.*
- *Featured image by marcos mayer on Unsplash*
- *When you leave a comment, you're agreeing to our Comment Policy*