‘Must Fix Trust’: Privacy-enhancing technologies as reductive tool

Tom Barbereau[1,2,*], Thijmen van Gend[1]

[1]*Dutch Organisation for Applied Scientific Research (TNO), Anna van Buerenplein 1, 2595 DA The Hague, The Netherlands*

[2]*Institute for Information Law (IViR), University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV Amsterdam, The Netherlands*

Abstract

Privacy-enhancing and other related digital technologies are marketed as increasing trust within the digital society. They are deployed as means to assert trust in digital transactions and interactions between actors. What this commentary argues is that digital trust is thereby reduced to the product of a technological iteration, insertion, or fix: more encryption $\simeq$ more privacy $\simeq$ more trust. However righteous it may be to foster privacy, the promise to uphold something as uncertain as trust by the use of mathematics and/or statistics alone is short-sighted. Lofty notions like ‘data minimisation’ and ‘privacy-by-design’ rest on deterministic assumptions. We suggest that in reductively appropriating the concept of trust and failing to meet expectations, the consequences of the technification of trust – i.e., the making of trust a product of *technê* (alone) – are paradoxical in that they actually undermine trust, by centralising power within tech companies.

Keywords

Trust, Determinism, Privacy-enhancing technologies

1. Introduction

Historical events have challenged our perceptions of trust – particularly, within the digital realm. From the Cambridge Analytica case and the extractive business of TikTok, to the Dutch childcare benefits scandal and the way we relied on Big Tech’s services during the Covid-19 pandemic, trust in the digital society has eroded.

In response to this erosion, organisations have turned to technological solutions, crafting compelling narratives. Zero-knowledge proofs (ZKPs) are applied to increase confidence in (digital) interactions; multi-party computation (MPC) is applied as security layer for sharing data (Agahari et al. 2022); federated learning beefed up with differential privacy is applied to reduce risk in collaborations (Fernandez et al. 2024); and so on. In each of these, “trust is tacitly equated with other terms which turn out to be the real focus”, observes Kroeger (2022). Privacy-preserving (or -enhancing) technologies (PETs) in particular are deployed to supposedly reduce users’ risk (i.e. the probability and impact of a privacy breach) and need for trust (i.e. “the need to rely on other entities to behave as expected”) (Gürses et al. 2015).

Position paper submitted to the Amsterdam Trust Summit 2025 on 19-02-2025, to be presented on 28-08-2025.

*Corresponding author.

tom.barbereau@tno.nl (T. Barbereau); thijmen.vangend@tno.nl (T. van Gend)

0000-0002-8554-0991 (T. Barbereau); 0000-0001-9157-9107 (T. van Gend)

Accordingly, these "trust technologies" (Chew et al. 2023; Ajish 2024)[1] are marketed as means to uphold trust by minimising used data, providing transparency, being private 'by-design', or creating 'zero trust' environments. Apple, Google, Amazon, et al. have appropriated the narrative of fixing trust by equating it to heightened privacy (e.g. Apple, n.d.; Patel 2023). Even the European Commission (2019) suggests that one can effectively "build" digital trust.

This commentary argues that the reduction of trust to the product of a process of technological adaptation, insertion, or what we describe as "fix" (Weinberg 1967) is itself problematic. After an introduction to the reductive appropriation of trust as concept, we argue that this reduction is a form of technological determinism or "solutionism" (Mann et al. 2022). Then, we turn to the consequences of this reduction in connection to the idea of a "cynical resignation" in the face of persistent centralisation of power (McGuigan et al. 2023). At last, in the form of an outlook, we point to alternatives to that centralisation.

2. Trust as fix

Scholars have discussed dimensions of trust and its role within societal systems, government, and so on. With the rise of large tech companies' infrastructures, online platforms, and 'e-Government,' they considered to what extent the very institutions within our digital society and economy became mediators (Bodó 2020) that provide infrastructures of trust (Bodó 2021). Technology is frequently associated with trust as it ought to provide "means and mechanisms that deliver predefined outputs reliably and predictably" (Chew et al. 2023). This mechanic, solutionist view on trust as fix is especially visible in cases where "trust is chosen as a label" to denote risk, confidence, or reliability (Kroeger 2022; Laux et al. 2024).

Leading the pack in this reductive appropriation are "promissory organisations" (Pollock and Williams 2010). McKinsey & Company define digital trust as the "confidence in an organization to protect consumer data, enact effective cybersecurity, offer trustworthy [...] products and services, and provide transparency" (Boehm et al. 2022). It deems digital trust a revenue generator by linking it to privacy and cybersecurity; improvement areas where shareholders can expect a return on investment (see also Kluiters et al. 2022) The World Economic Forum, in a commissioned survey-based study, claims that even a "5% point increase in digital trust results in an average increase in GDP per capita of $3000" (Hayat 2022).

The technical literature underpins these reductive claims through empirics. A quick analysis of Scopus records mentioning 'digital trust' published at ACM and IEEE from 2000-2024[2] (Figure 1) indicates that digital trust has crept into technical scholarship. From that sample, selected at random, works equate some technologies with trust: Ganescu and Passerat-Palmbach (2024) claim that "applying ZKPs to machine learning models [...] enables independent validation [...], promoting transparency and trust". Agahari et al. (2022) suggest that MPC provides "higher control over data through technology-based control [and] lower the need for trust in other actors involved". Yang et al. (2024) find that "differential privacy [...] eliminates the need for a

[1] We cynically appropriate this umbrella term to refer to a complete suite of technologies. It includes privacy-enhancing technologies (PETs) mentioned above; as well as blockchain and specific identity systems. For a taxonomy to be taken with a grain of salt, refer to Lam (2023).

[2] Restricted to mentions in the title, abstract, or keywords in journal articles.

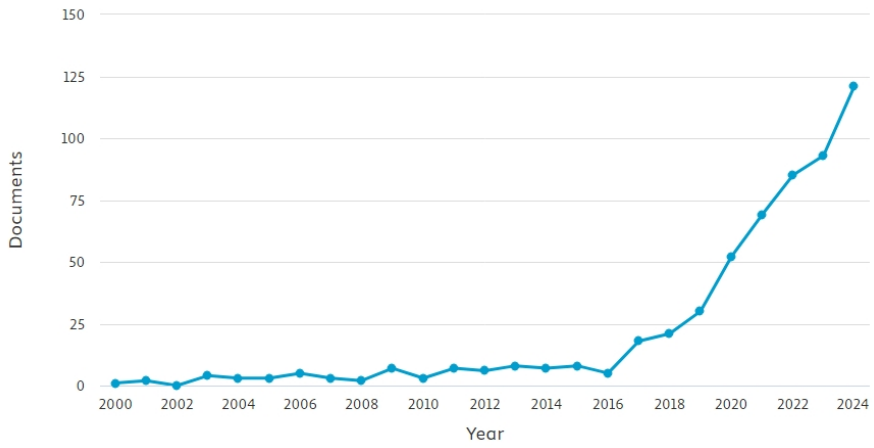

Figure 1: Result of Scopus document analysis.

trusted third party". Veale (2023b) concludes that PETs specifically are frequently posited as technological fixes to problems. This, even in cases where it may not be desirable.

Big Tech commonly, in their myriad of services, adopts the rhetoric that links privacy with trust. Examples include Google's "privacy-first" digital advertising services (Patel 2023; Temkin 2021); "safe and trusted" app stores (Apple, n.d.); mobile payment services by Apple (2024a) that "protect users' highly sensitive personal and financial information" and give "peace of mind"; Amazon's smart-home devices that "build and maintain trust for millions of customers" (Kellner and Wilhelm 2023); "secure, compliant, and privacy-focused cloud services" to "earn and maintain your trust" by Microsoft (2024);[3] and, GenAI services that unlock "intelligence users can trust" (Apple 2024b) or that come with a "Trust Portal" as "gateway to [the] unwavering commitment to data security, privacy, and compliance" (OpenAI, n.d.).

These various examples from promissory organisations, technical literature, and Big Tech, effectively reduce trust to a measurable outcome; positioning (most frequently, privacy-enhancing) technology as a fix, a "social cure-all" (Johnston 2018) that creeps into systems (Koops 2021). This is textbook solutionism (Mann et al. 2022) – the premise upon which we see a number of critiques arising.

3. Critiques and quandaries

Our position vis-à-vis the 'technology as fix to trust' narrative regurgitated by promissory organisations, engineers, and Big Tech alike, follows extensive dissections put forward by critical scholars. First, we point to a stream of literature on the unique position that large tech companies have to roll out services and products – in the domains of digital advertising (Veale 2023a), payments (Canepa 2022), cloud services (Rikap 2024; Vlist et al. 2024), amongst others. The literature points to the continued dogma of profit maximisation in the process of deploying PETs. The logic that equates trust with privacy is doubtful; a "cynical resignation"

[3] Also Amazon (2022).

as "companies concede that they must react to new laws and cultural norms" while resorting to technical solutions that "aim to reproduce the status quo or even justify anticompetitive behaviour" (McGuigan et al. 2023). Thus, deploying PETs may not limit extractive practices.

Second, Veale (2023a) observes that "encryption goes from a narrow set of tools to an infrastructure". For instance, encryption used to be discussed with relation to specific forms of communication (e.g. phone calls and chats). Debates around encryption (and therefore, PETs) focused on the purposes of communication: proponents of encryption advocated for freedom of expression regardless of content, opponents warned of child pornography and crime. Today, PETs encrypt all kinds of computation and data analyses – and with that entire business models. This "quickly, and confusingly, blur[s] personal privacy and corporate opacity", while ironically opening up avenues for advertising based on even more sensitive user data (Veale 2023a).

Third, Big Tech companies strategically leverages PETs to *entrench* their infrastructure in how other organisations deliver their services. Google and Apple rolled out PET-based device finding (e.g., Apple Find My) and digital advertising services (e.g., Google's Privacy Sandbox and Apple's App Tracking Transparency); putting their own infrastructure at the heart of competitors' services (van Gend et al. 2024). Similarly, in rolling out a purportedly privacy-preserving technology for Covid-19 contact tracing, Apple and Google claimed governmental decision-making power from public institutions (Troncoso et al. 2022). In another example, Amazon repurposed consumers' smart-home devices to offer a crowdsourced network that third-party devices can connect to – requiring manufacturers of said devices to align themselves with Amazon's propagated norms of trust; i.e., requirements for device hardware and software (van Gend et al. 2024).[4] These services each rely on the participation of millions of consumer devices. The companies use PETs to justify creating new information flows, blocking competing technologies, and/or enabling them by default.

We conclude with the sum of these critiques. Big Tech companies leverage PETs in a way that actually aggravates power asymmetries. While claiming to solve trust claims with PETs, issues are repackaged. These two facets constitute a "PET Paradox" (van Gend et al. 2024). Central hereto is that many systems centralise key functions pertaining to network information and computation, and trust propagation to certain parties (Troncoso et al. 2017).

4. Outlook

We argue for caution in attempts to fix trust with technology alone. We pointed to the well-known, centralising forces that repackaging trust through technology brings about, in turn aggravating power asymmetries instead of resolving systemic issues of the digital realm. We advocate for further study into these issues and encourage the consideration of alternatives. We provide an outlook by shedding light on some proposals.

Masnick (2019) argues for "a world where protocols and not proprietary platforms dominate". In his vision, users access digital services through implementations and interfaces built on top of a protocol; as is the case with email. Moderation and content curation powers would not lie with only one company, but with those that make rules and interfaces for these protocols.

[4] Generally, Amazon has been particularly successful to lock products and services into their cloud (Rikap 2020; Vlist et al. 2024).

Users can then choose between 'competing' implementations and further tailor these. Bria (2024) and other 'EuroStack' advocates argue that the EU should stimulate initiatives for public tools, services, and protocols across the technology stack, that "protect citizens' rights [...] and serve the public interest". This stimulation entails targeted subsidies; encouraging early adoption by public bodies; and including conditions in procurement that align with public values. Similarly, Rikap et al. (2024) propose a roadmap for "a democratic, public-led digital stack [...] provided by non-profit and democratic international consortia". This includes "universal platforms [...] that should be a commons governed by new public institutions with state and civil society representation" and a public marketplace for lock-in-free services, that states should also procure from.

While assessing their scopes, definitions, and epistemologies is outside the scope here, we encourage future work to engage with the issues this paper pointed out.

Acknowledgments

The authors thank Ilina Georgieva and Gabriela Bodea for their reviews. The views reflected in this work do not necessarily represent those of TNO.

References

Agahari, Wirawan, Hosea Ofe, and Mark de Reuver. 2022. "It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing." *Electronic Markets* 32 (3): 1577–1602. ISSN: 1422-8890. https://doi.org/10.1007/s12525-022-00572-w.

Ajish, Deepa. 2024. "The significance of artificial intelligence in zero trust technologies: a comprehensive review." *Journal of Electrical Systems and Information Technology* 11 (1): 30–23. ISSN: 2314-7172. https://doi.org/10.1186/s43067-024-00155-z.

Amazon. 2022. *Amazon Is Earning and Maintaining Customer Trust through Privacy.* Accessed January 15, 2025. https://www.aboutamazon.com/news/how-amazon-works/amazon-is-earning-and-maintaining-customer-trust-through-privacy.

Apple. 2024a. *Apple Celebrates 10 Years of Apple Pay.* Accessed January 15, 2025. https://www.apple.com/newsroom/2024/10/apple-celebrates-10-years-of-apple-pay/.

———. 2024b. *Introducing Apple Intelligence, the Personal Intelligence System That Puts Powerful Generative Models at the Core of iPhone, iPad, and Mac.* Accessed January 15, 2025. https://www.apple.com/newsroom/2024/06/introducing-apple-intelligence-for-iphone-ipad-and-mac/.

———. n.d. *User Privacy and Data Use.* Accessed January 15, 2025. https://developer.apple.com/app-store/user-privacy-and-data-use/.

Bodó, Balázs. 2020. "Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators." *New Media & Society* 23 (9): 2668–2690. ISSN: 1461-4448. https://doi.org/10.1177/1461444820939922.

———. 2021. "The Commodification of Trust." *Amsterdam Law School Research Paper,* no. 22, https://doi.org/10.2139/ssrn.3843707.

Boehm, Jim, Liz Grennan, Alex Singla, and Kate Smaje. 2022. *Why digital trust truly matters.* Technical report. McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters.

Bria, Francesca. 2024. *The Quest for European Technological Sovereignty: Building the EuroStack,* October. Accessed January 22, 2025. https://techpolicy.press/the-quest-for-european-technological-sovereignty-building-the-eurostack.

Canepa, Allegra. 2022. "The Role of Payment Services in the Development of the Big Tech Ecosystem." *European Business Law Review* 33 (7). ISSN: 0959-6941. https://doi.org/10.54648/eulr2022043.

Chew, H.E., J. Tan, and C. Soon. 2023. "Digital Trust and Why It Matters." *NUS-CTIC Working Paper Series,* https://ctic.nus.edu.sg/resources/CTIC-WP-05(2023).pdf.

European Commission. 2019. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence,* COM(2019) 168. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0168.

Fernandez, Joaquin Delgado, Renan Lima Baima, Tom Barbereau, and Alexander Rieger. 2024. "Opportunities and Applications of Federated Learning in the Financial Services Industry." In *Decentralization Technologies: Financial Sector in Change,* 195–213. Springer. ISBN: 978-3-031-66047-4. https://doi.org/10.1007/978-3-031-66047-4_11.

Ganescu, Bianca-Mihaela, and Jonathan Passerat-Palmbach. 2024. "Trust the Process: Zero-Knowledge Machine Learning to Enhance Trust in Generative AI Interactions." *ArXiv e-prints,* https://doi.org/10.48550/arXiv.2402.06414.

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 2015. "Engineering Privacy by Design Reloaded." In *Amsterdam Privacy Conference 2015.* Amsterdam, The Netherlands. https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf.

Hayat, Zia. 2022. *Why digital trust is key to building thriving economies.* Technical report. World Economic Forum. https://www.weforum.org/stories/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy.

Johnston, Sean F. 2018. "The Technological Fix as Social Cure-All: Origins and Implications." *IEEE Technology and Society Magazine* 37 (1): 47–54. https://doi.org/10.1109/MTS.2018.2795118.

Kellner, Tomas, and Henry Wilhelm. 2023. *How Amazon Builds Its Devices with Your Privacy in Mind.* Accessed January 15, 2025. https://www.aboutamazon.com/news/devices/how-amazon-builds-its-devices-with-your-privacy-in-mind.

Kluiters, Leon, Mohit Srivastava, and Ladislav Tyll. 2022. "The impact of digital trust on firm value and governance: an empirical investigation of US firms." *Society and Business Review* 18 (1): 71–103. https://doi.org/10.1108/SBR-07-2021-0119.

Koops, Bert-Jaap. 2021. "The concept of function creep." *Law, Innovation and Technology* 13 (1). https://doi.org/10.1080/17579961.2021.1898299.

Kroeger, Frens. 2022. "What is trust in technology? Conceptual bases, common pitfalls and the contribution of trust research." In *Trust & Technology Initiative: Research Perspectives.* University of Cambridge. https://www.trusttech.cam.ac.uk/perspectives/technology-humanity-society-democracy/what-trust-technology-conceptual-bases-common.

Lam, Kwok. 2023. *Digital Trust Centre Research Grant Call presentation.* [Slide 8]. https://www.ntu.edu.sg/docs/ncdtlibraries/research-grant-call/2023-07-17-dtc-research-grant-call-briefing-slides.pdf?sfvrsn=f60f0e68_3.

Laux, Johann, Sandra Wachter, and Brent Mittelstadt. 2024. "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk." *Regulation & Governance* 18, no. 1 (January): 3–32. ISSN: 1748-5983. https://doi.org/10.1111/rego.12512.

Mann, Monique, Peta Mitchell, and Marcus Foth. 2022. "Between surveillance and technological solutionism: A critique of privacy-preserving apps for COVID-19 contact-tracing." *New Media & Society* 26 (7): 4099–4117. ISSN: 1461-4448. https://doi.org/10.1177/14614448221109800.

Masnick, Mike. 2019. *Protocols, Not Platforms: A Technological Approach to Free Speech.* Technical report. Knight First Amendment Institute, August. Accessed January 22, 2025. http://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech.

McGuigan, Lee, Sarah Myers West, Ido Sivan-Sevilla, and Patrick Parham. 2023. "The after party: Cynical resignation in Adtech's pivot to privacy." *Big Data & Society* 10 (2): 20539517231203665. ISSN: 2053-9517. https://doi.org/10.1177/20539517231203665.

Microsoft. 2024. *Microsoft Cloud for Sovereignty*. Accessed January 16, 2025. https://learn.microsoft.com/en-us/industry/sovereignty/sovereignty-capabilities.

OpenAI. n.d. *OpenAI Security Portal.* Accessed January 16, 2025. https://trust.openai.com/.

Patel, Peentoo. 2023. *Get to Know Our Privacy and Data Tools.* https://blog.google/products/admanager/get-to-know-our-privacy-and-data-tools/.

Pollock, Neil, and Robin Williams. 2010. "The business of expectations: How promissory organizations shape technology and innovation." *Social Studies of Science* 40 (4): 525–548. https://doi.org/10.1177/0306312710362275.

Rikap, Cecilia. 2020. "Amazon: A story of accumulation through intellectual rentiership and predation." *Competition & Change* 26, nos. 3-4 (June): 436–466. ISSN: 1024-5294. https://doi.org/10.1177/1024529420932418.

———. 2024. "Varieties of corporate innovation systems and their interplay with global and national systems: Amazon, Facebook, Google and Microsoft's strategies to produce and appropriate artificial intelligence." *Review of International Political Economy,* ISSN: 0969-2290. https://doi.org/10.1080/09692290.2024.2365757.

Rikap, Cecilia, Cédric Durand, Edemilson Paraná, Paolo Gerbaudo, and Paris Marx. 2024. *Reclaiming Digital Sovereignty: A Roadmap to Build a Digital Stack for People and the Planet.* Technical report. LUT University, December. https://lutpub.lut.fi/handle/10024/168600.

Temkin, David. 2021. *Charting a Course towards a More Privacy-First Web.* https://blog.google/products/ads-commerce/a-more-privacy-first-web/.

Troncoso, Carmela, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda Gürses, Jean-Pierre Hubaux, et al. 2022. "Deploying Decentralized, Privacy-Preserving Proximity Tracing." *Communications of the ACM* 65 (9): 48–57. ISSN: 0001-0782. https://doi.org/10.1145/3524107.

Troncoso, Carmela, Marios Isaakidis, George Danezis, and Harry Halpin. 2017. "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments." *Proceedings on Privacy Enhancing Technologies* 2017, no. 4 (June): 404–426. ISSN: 2299-0984. https://doi.org/10.1515/popets-2017-0056.

van Gend, Thijmen, Donald Jay Bertulfo, and Seda Gürses. 2024. *The PET Paradox: How Amazon Instrumentalises PETs in Sidewalk to Entrench Its Infrastructural Power.* https://doi.org/10.48550/arXiv.2412.09994.

Veale, Michael. 2023a. "Confidentiality Washing in Online Advertising." In *Eaten by the Internet,* edited by Corinne Cath, 43–48. Amsterdam, The Netherlands: Meatspace Press. ISBN: 978-1-913824-05-1. https://archive.org/details/eaten-by-the-internet.

———. 2023b. "Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!" In *The Person and the Future of Private Law,* edited by Hans-Wolfgang Micklitz and Giussepe Vettori. Forthcoming. Hart. https://doi.org/10.31235/osf.io/4ugxd.

Vlist, Fernando van der, Anne Helmond, and Fabian Ferrari. 2024. "Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence." *Big Data & Society* 11, no. 1 (March): 20539517241232630. ISSN: 2053-9517. https://doi.org/10.1177/20539517241232630.

Weinberg, Alvin M. 1967. "Can Technology Replace Social Engineering?" *American Behavioral Scientist* 10 (9): 7. ISSN: 0002-7642. https://doi.org/10.1177/0002764201000903.

Yang, Mengmeng, Taolin Guo, Tianqing Zhu, Ivan Tjuawinata, Jun Zhao, and Kwok-Yan Lam. 2024. "Local differential privacy and its applications: A comprehensive survey." *Computer Standards & Interfaces* 89 (April): 103827. ISSN: 0920-5489. https://doi.org/10.1016/j.csi.2023.103827.