‘Must Fix Trust’

Privacy-enhancing technologies as reductive tools

Amsterdam Trust Summit
28 August 2025

Tom Barbereau

Thijmen van Gend

TNO Vector

State of affairs

Privacy-enhancing technologies

Repackaging through adaptation

Turn to technological solutions

Trust technologies
Uphold trust by minimising used data, providing (some) transparency, being private 'by-design', or creating 'zero trust' environments.

Appropriation

Trust has eroded

Cambridge Analytica

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.

Trust as fix

Technology is frequently associated with trust: 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).

Technical literature	**Promissory organisations**	**Big Tech**
think engineering, computer science, cryptography, et al.	think McKinsey & Company, the World Economic Forum et al.	think Apple, Microsoft, Google, Meta, OpenAI et al.
“Zero knowledge [...] promotes transparency and trust”, “MPC [...] lowers the need for trust”, “differential privacy [...] eliminates the trusted third party”	digital trust as revenue generator by linking it to privacy and cybersecurity; improvement areas where shareholders can expect a return on investment (Kluiters et al. 2022)	“Safe and trusted” app stores, “privacy first” digital advertising, “earn and maintain trust” in communication, “Trust Portal” for security, privacy, and compliance

Recent cases

1. Transactiemonitoring Nederland

Multi-party computation for money laundering detection

2. Digital identities & age verification

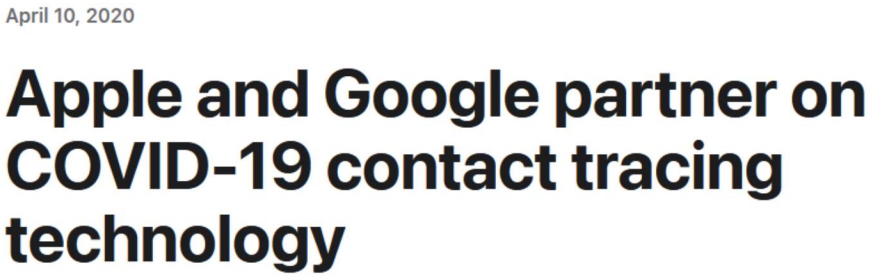
Zero-knowledge proofs and more to prove age, identity

3. CSAM detection

Client-side scanning by Apple

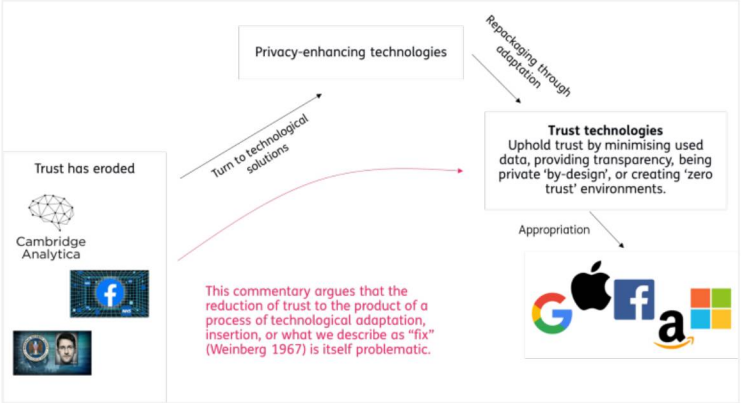
4. Digital contact tracing during Covid-19

Privacy-preserving API by Google and Apple



Critiques and quandaries

These various examples 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). Arguably, this is textbook solutionism (Mann et al. 2022).



Trust is a necessary point of discussion in the context of PETs.

Remember: PETs in principle aim to eliminate the need for trust

Big tech companies **entrench their infrastructures** in vital sectors	Not eliminating, but **reconfiguring the need for trust**	**Normalization to establish “trustworthiness”**, online and in-person
– Reshaping how governments and companies can ‘produce’ (public) services – We should be mindful of centralising forces in (decentralised) trust techs (van Gend et al. 2024)	– Big tech companies cement themselves in public services – We must trust that technologies (often depicted as ‘magical’) are properly designed, implemented, and governed	– Yes, PETs allow for more privacy-preserving attestation… but the status quo is not flashing your passport everywhere – Does distrust in users warrant subjecting everyone to age verification schemes?

Thank you!

References provided in this presentation are provided in the manuscript. The opinions presented in this work do not necessarily reflect those of TNO.