Toward a Multi-Dimensional Valuation of Personal Data in the Digital Economy

Keywords: Personal data valuation; Network risk; Data breaches; Complexity economics; Privacy harm

Extended Abstract

In the digital economy, personal data acts as both a critical resource and a systemic vulnerability. Organisations across sector - from social media to retail - depend on interconnected information flows to personalise services, optimise operations, and generate insights. These interlinked data assets create significant economic value but also embed individuals within networks of risk where breaches can propagate through financial, technological, and social systems.

Traditional approaches to valuing personal data rely primarily on aggregate market statistics, producing coarse-grained estimates that often neglect individual harms, network effects, and systemic consequences. For instance, most market-based valuations do not account for (i) non-linear escalation of risk as multiple attributes of a single person become linked, (ii) cumulative downstream effects that ripple through interconnected systems, or (iii) the ethical costs of diminished trust and inequitable distribution of harm. This undervaluation distorts both organisational risk management and the frameworks of redress for individuals.

We propose a multi-source, fine-grained valuation model that integrates economic, legal, and network-science perspectives. Our framework combines market-based measures with harm-based assessments (including willingness-to-pay approaches and litigation outcomes) while explicitly modelling interdependencies as multilayer networks. By embedding individual data points within network structures, the model captures how the compromise of a few attributes can cascade into disproportionate losses across identity, financial, and social domains.

The methodology draws on administrative microdata (e.g., New Zealand's Integrated Data Infrastructure) linked with macroeconomic indicators (from StatsNZ) to produce scalable estimates. At the micro level, we model escalation functions of individual harm based on empirical findings from contingent valuation studies and breach litigation outcomes. At the meso-level, organisational exposure is modelled through network centrality measures, capturing dependencies across firms and sectors. At the macro level, national risk is assessed by aggregating these measures and simulating systemic shocks under different breach scenarios.

Preliminary findings suggest that conventional valuations understate damage by at least an order of magnitude, particularly when considering cascading effects across sectors such as finance and healthcare. For example, empirical analyses of privacy breaches show market losses averaging hundreds of millions of dollars, yet these figures omit long-term consumer trust erosion, litigation costs, and spillovers to competitors. A network-based approach allows us to more fully capture these hidden costs, offering a more accurate and socially responsive valuation.

Ethical considerations

This work directly engages with questions of privacy, fairness, and data sovereignty. In the Aotearoa New Zealand context, the use of administrative microdata requires strict adherence to privacy safeguards and alignment with Māori data sovereignty principles. More broadly, we acknowledge that valuation models can be misused by insurers or employers to commodify personal risk; therefore, transparency in methodology and safeguards against exploitative applications are essential. Our framework is designed not to monetise individuals, but to correct distortions that currently undervalue harm and under-protect those affected by data breaches.

By reframing personal data within a network science perspective, this research contributes to understanding how value and risk emerge, interact, and amplify in connected systems. It provides complexity-aware tools for organisational governance, public policy, and individual redress, advancing both the economics of privacy and the ethics of data use.

References

[1] Acquisti, A. (2010). *The Economics of Personal Data and the Economics of Privacy.* CMU Heinz College.

[2] Lee, S.Y., Chung, J.H., & Lee, J.S. (2015). *A study on the damage costs for private information leakage using the contingent valuation method.* WIT Transactions on The Built Environment, 168.

[3] Romanosky, S., Hoffman, D., & Acquisti, A. (2013). *Empirical Analysis of Data Breach Litigation.*

[4] Tao, H., Bhuiyan, M.Z.A., Rahman, M.A., et al. (2019). *Economic perspective analysis of protecting big data security and privacy.* Future Generation Computer Systems, 98, 660–671.

[5] Tripathi, M., & Mukhopadhyay, A. (2020). *Financial Loss due to a Data Privacy Breach: An Empirical Analysis.* Journal of Organizational Computing and Electronic Commerce.

Disclaimer

ChatGPT has been used to correct any grammatical error and for minor editorial changes in the draft.

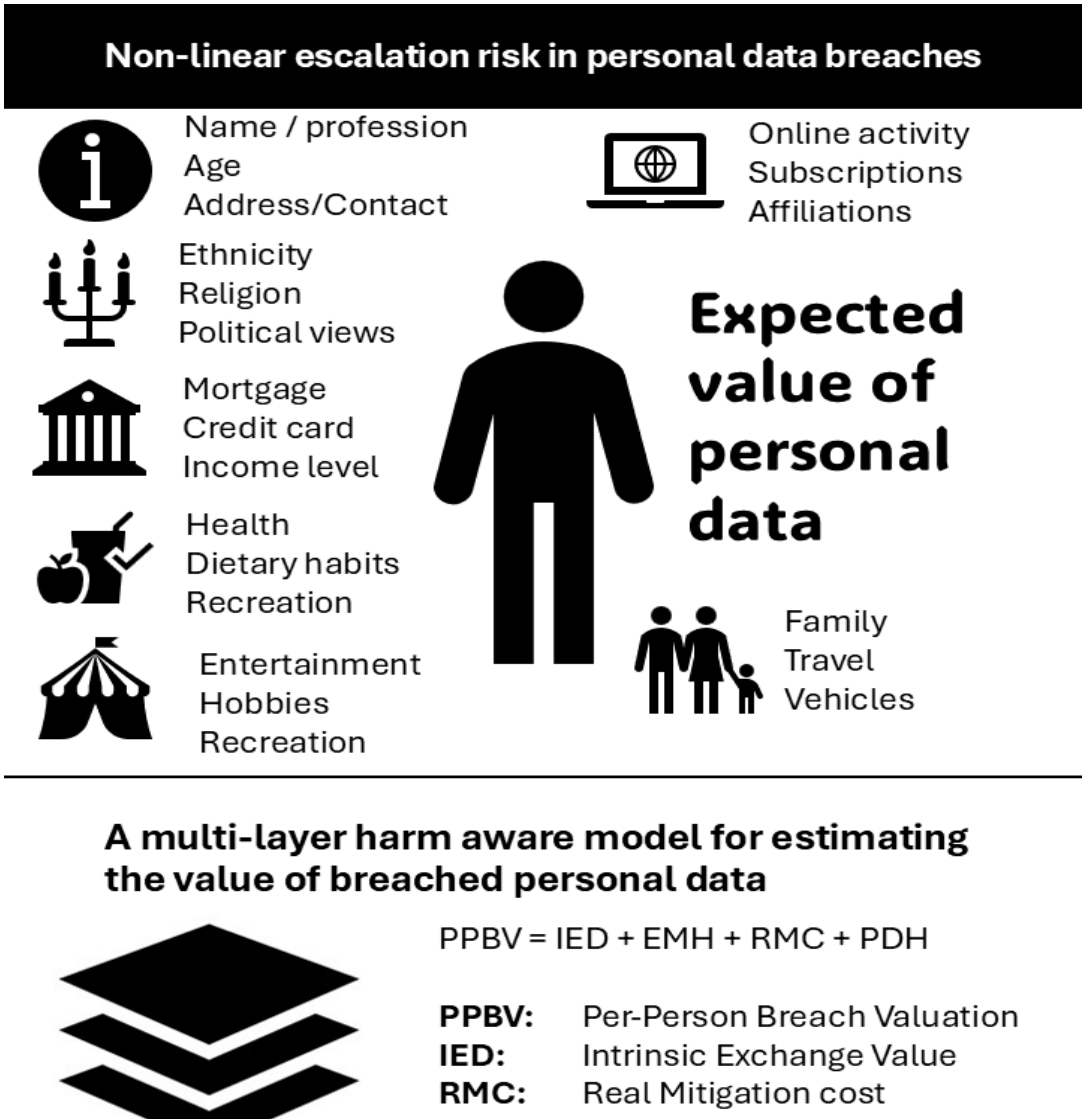

Figure 1. **Concept framework.** This is a work in progress.