Jovan Powar

Google Scholar
jovan@powarup.com

AI governance researcher focused on how emerging technologies are deployed and governed in practice, and how governance frameworks integrating technical and non-technical mechanisms can address their risks. Experience in structured risk analysis and cross-disciplinary engagement with technical security, legal, and policy communities, and translating findings into actionable outputs for practitioners and policymakers.

At the Alan Turing institute, led research on GenAI risk management and governance within major financial institutions. PhD research at Cambridge (awaiting viva) focused on bridging technical privacy research with risk-based data protection, and risk management approaches that incorporate technical and non-technical mitigations. Currently: co-leading research on participatory data and AI governance, examining how structural models of governance can enable data usage with stronger accountability; and participating in AI Governance Sprint on incident reporting.

Experience & education

Alan Turing Institute

Researcher, FAIR programme **2023 – 2026**

Led Partnership on AI in Finance research project on **Model Risk Management and Governance for GenAI in financial services**:

- Lead author of *GenAI Model Risk Management and Governance in Financial Services: From Principles to Practice*, practitioner-facing guidance synthesising how five major financial institutions understand and govern frontier AI risk, with concrete recommendations on risk elicitation and oversight for GenAI deployment.
- Designed and led structured workshops and expert interviews to surface how practitioners understand and manage frontier AI risk—translating diverse institutional perspectives into a coherent cross-sector evidence base.

Holistic risk & security analysis of a privacy-preserving cross-border system for a major international bank:

- Extended STRIDE threat modelling to disclosure-specific risks, analysing threats at system-level and at trust boundaries
- Worked with development, operations, and compliance teams to establish scope and delivered report used as reference for ongoing R&D and decision-making

Participatory data governance

Co-lead, research project & community of practice **ONGOING**

Co-leading work with colleagues at UC Berkeley on participatory data and AI governance through workshops, community-building, and writing on structural governance models. Researching how governance structures and institutional design shape accountability in practice.

Led workshop **"Participatory Data Governance in Practice" @ ACM CHI 2026**.

University of Cambridge

PhD candidate **OCT 2017 – JUN 2021 (FAMILY LEAVE HIATUS) EXP. GRAD. H1 2026**

Thesis: **Data protection as risk management**, under Prof. Alastair Beresford & Dr Jat Singh. Research develops cross-disciplinary approaches to governing socio-technical data systems under uncertainty in open real-world contexts, including:

- Risk-based privacy threat modelling framework (**SoK paper @ PETS 2023**)
- Integrating technical protection with data governance and structural controls such as data intermediaries (**paper @ FAccT 2025**)
- Interdisciplinary critique of **-by-Design* regulatory guidance frameworks, engaging with legal scholarship (**workshop paper @ PLSC Europe 2024**)

CompSci BA, MEng with Distinction **2012 – 2017**

Rethinking Data

Technical brief for Ada Lovelace Institute **2021**

Commissioned analysis providing background and briefing on emerging data technologies for ALI's Rethinking Data working group.

Skills

Familiar with risk management and governance frameworks including NIST AI RMF, the EU AI Act, financial Model Risk Management (SR 11-7, SS1/23), frontier AI risk frameworks, and data protection.

Strong public speaker and writer with experience presenting research and leading panels for technical and non-technical audiences.

Experienced in cross-disciplinary stakeholder engagement and collaboration on co-authored outputs.

Strong technical grounding in privacy-enhancing technologies and information security, with practical software engineering experience across research and applied projects (incl. Python, Java, LangChain).

Comfortable engaging with legal scholarship, policy, and governance frameworks, including presenting at PLSC Europe 2024, attending IVIR summer school on data protection law, engaging with policy scholars.

Selected Publications

GenAI Model Risk Management and Governance in Financial Services: From Principles to Practice — 2025 Turing report

SoK: managing risks of linkage attacks on dataset privacy — PETS 2023

From policy to practice in data governance and responsible data stewardship: system design for data intermediaries — FAccT 2025