IOCSS 2026 Conference
The 1st International Online Conference on Social Sciences
28–29 May 2026 | Online
MDPI

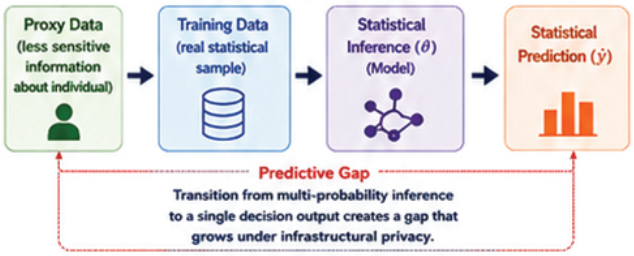
Privacy Curtain; Sacrificing Causal Inference in Predictive Systems? Revisiting Value Conflict from a Modern Paradox

Dr. Hojjat Kazemi, Seyed Amir Iravani
University of Tehran, Faculty of Law and Political Science, 16th Azar St., Enghelab Sq., Tehran, Islamic Republic of Iran
Hkazemi57@ut.ac.ir | Amir.Iravani@ut.ac.ir

INTRODUCTION & AIM

- Machine learning–based predictive systems (PS) infer target behaviors of individuals using proxy data embedded in causal relationships learned from training data.
- Privacy protection techniques (e.g., anonymization, perturbation) create a "privacy curtain" that deviates data from authenticity.
- Our aim is to examine how infrastructural privacy conflicts with causal inference, increases the predictive gap, and leads to systematic bias in intelligent automation.

THE INFERENCE PIPELINE



REAL-WORLD EXAMPLES

A. American Supermarkets
Used purchase data to identify pregnant customers; led to high false positives/negatives due to incomplete sampling and poor data quality, raising ethical and privacy concerns.

B. Terrorism Identification
U.S. "Skynet" project analyzed 55 million mobile users' metadata in Pakistan; a false positive rate of 0.008% still flagged ~15,000 individuals incorrectly.

METHOD

LITERATURE REVIEW APPROACH

A hybrid review was conducted across Scopus, IEEE, and Google Scholar (2019–2025) using keywords: "Machine Learning", "Model Accuracy", "Privacy". 21 sources were analyzed.

Horizontal (Domain) Review
Interdisciplinary coverage of:
- Predictive privacy
- Big data & challenges
- Synthetic data generation
- Differential privacy in modeling
- Intelligent automation & bias

Vertical (In-Depth) Review
Value conflict analysis inspired by:
- Max Weber: methodology & value rationality
- Isaiah Berlin: value pluralism
- Sociological understanding of techno-social systems

FINDINGS FROM CODE ANALYSIS (21 ARTICLES)

Model Accuracy Metrics	Automation (RPA / IA)	Systemic Discrimination	Infrastructural Privacy (GDPR/CCPA, etc.)	Social Science Coverage
ROC/AUC, MSE, MAE, etc.) 81%	62%	43%	48%	14%

GAPS IDENTIFIED

1. Lack of integration of these six concepts within social sciences.
2. Need for multidimensional evaluation methods.
3. Large gap between technical solutions and social considerations.
4. The relationship between privacy and model accuracy hasn't been examined.

RESULTS & DISCUSSION

THE VICIOUS CYCLE OF TECHNICISM

INFRASTRUCTURAL PRIVACY: OBJECTIVE APPLICATION PATTERNS

A. Differential Privacy

$$P[M(D) \in S] \leq e^{\varepsilon} P[M(D') \in S]$$

- Adds controlled noise to data/outputs.
- ε (privacy budget): smaller $\varepsilon \rightarrow$ stronger privacy, lower accuracy.
- Causes deviation from authentic data (primary signals).

B. Synthetic Data Paradigm
Artificially generated data that imitate real data distributions.
- No generator simultaneously optimizes utility, privacy, and fairness.
- Leads to biased or distorted causal relationships.

IMPLICATIONS: FROM PREDICTIVE GAP TO SYSTEMATIC BIAS

Infrastructural Privacy → Increased Predictive Gap → Intelligent Automation → Systematic Bias

- Errors in micro-level predictions aggregate into macro-level policies.
- Unrealistic and potentially harmful outcomes, especially in high-stakes domains (e.g., healthcare, law enforcement, justice, finance).

DISCUSSION: VALUE CONFLICT PERSPECTIVE

- Following Weber and Berlin, privacy vs. accuracy is a value conflict, not a purely technical problem.
- Technicism reduces value conflicts to technical issues, causing a vicious cycle.
- Science tests the feasibility of trade-offs but does not eliminate the tragedy of choice.
- Context-sensitive, value-based judgments are required to balance competing values.

CONCLUSION

- Infrastructural privacy—rooted in technicism and data perturbation—inevitably deviates data from authenticity.
- This deviation increases the predictive gap and results in systematic bias when applied in intelligent automation.
- Technical solutions alone cannot resolve the privacy–accuracy paradox; value-aware trade-offs are essential.
- Balanced, context-sensitive policies are needed to protect privacy while maintaining reliable, fair predictive systems.

REFERENCES

- Weber, M. (1949). The methodology of the social sciences. Free Press.
- Weber, M. (2019). Economy and society: A new translation. Harvard University Press.
- Berlin, I. (2018). The lessons of history. In *The Cambridge companion to Isaiah Berlin*. Cambridge University Press.
- Moorthy, J., et al. (2015). Big data: Prospects and challenges. *Vikalpa*, 40(1), 74–96.
- Galloway, K. (2017). Big data: A case study of disruption and government power. *Alternative Law Journal*, 42(2), 89–95.
- Mühlhoff, R. (2021). Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology*, 23(4), 675–690.
- Xiong, F., et al. (2022). Recognition and evaluation of data as intangible assets. *SAGE Open*, 12(2).
- Cummings, R., & Desai, D. (2018). The role of differential privacy in GDPR compliance. *FATREC 2018*.
- Khadka, K., et al. (2024). A combinatorial approach to hyperparameter optimization. *AI Engineering* (ICAI-SE), 140–149.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *FAT**, 77–91.
- Coombs, C., et al. (2020). The strategic impacts of intelligent automation. *J. Strategic Inf. Syst.*, 29(4), 101600.
- Liu, Y., Acharya, U. R., & Tan, J. H. (2025). Privacy in healthcare: Synthetic data generation review. *Comput. Methods Programs Biomedicine*, 260, 108571.
- Kiran, A., & Kumar, S. S. (2024). A methodology to determine the most suitable synthetic data generator. *IEEE Access*, 12, 12209–12228.
- Eponeshnikov, A., et al. (2023). Balancing accuracy, fairness and privacy in ML. *Adv. Syst. Sci. Appl.*, 23(4), 41–59.
- McKendrick, K. (2019). Artificial intelligence prediction and counterterrorism. Chatham House.
- Arnold, C., et al. (2024). The role of hyperparameters in machine learning models. *PSRM*, 12(4), 841–848.
- Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of AI and big data. *Big Data & Society*, 10(1).