Longitudinal Analysis of Meta privacy policy based on CI framework

Chengyuan Liang[1], Yan Shvartzshnaider[1]
[1]York University

Motivation

The introduction of AI technology has fundamentally transformed platform data processing models:

AI-driven information handling practice: deep learning optimization (Sarker, 2021) and real-time intelligent computing systems (Paramesha et al., 2024)

This marks a critical shift in the role of the "platform." Platforms have evolved from mere "data controllers" (determining collection purposes and methods) to active "data processors" (engaging in mining, analysis, and redistribution). While GDPR (Articles 13, 14) and EU AI Act (Articles 53, 54) set explicit disclosure requirements that platforms primarily fulfill through privacy policies (EDPB, 2018), current policies exhibit structural deficiencies: they detail basic data collection while inadequately disclosing AI's complex data processing models, severely undermining the effectiveness of regulatory assessment mechanisms.

Methodology

This study adopts the Contextual Integrity (CI) framework as its theoretical foundation (Nissenbaum, 2004). The CI framework defines privacy as the appropriateness of information flow, assessing privacy policies by identifying five key parameters in information flow (sender, recipient, subject, attribution, and transmission principle).

We capture the information handling practices prescribed in the privacy policy and other privacy related documentation to evaluate how they evolve throughout overtime, before and after the introduction of AI-based capabilities.

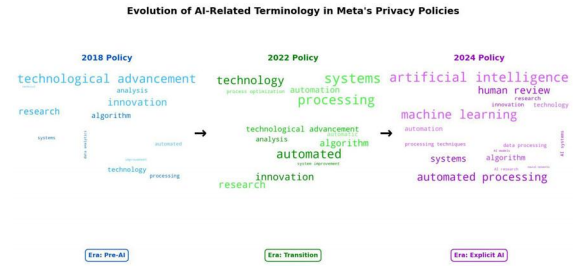
Privacy as an **appropriate information flow**

<actors*: subject, sender, recipient>, <attributes*>, <transmission principle>

Research Objective

This research establishes a joint framework for privacy policy analysis and legal compliance assessment, based on three key observations:

1. Expanded Data Usage Scenarios: AI has extended data use from basic business to autonomous decision systems and neural network training (Paramesha et al., 2024), yet privacy policies exhibit systematic disclosure inadequacies
2. Regulatory Trigger Points: 2023-2024 data shows regulatory actions against major platforms are predominantly triggered by privacy policy changes (IAPP, 2024), indicating policies as critical regulatory scrutiny starting points
3. Informed Consent Crisis: AI training poses unprecedented challenges to the informed-consent model, with platforms' freedom to arbitrarily adjust disclosure language further exacerbating this dilemma
4. Through longitudinal analysis of Meta's privacy policies, this research will reveal the complex relationships between platform role evolution, data use scope expansion, and existing regulatory framework adaptability.



Improved CI Parameter Comparison Table

CI Parameter	2018 Policy	2022 Policy	2024 Policy	Evolution Trend
Sender	"We" (Meta) ✅ Clear identification	"We" (Meta) ✅ Clear identification	"We" (Meta) ✅ Clear identification	**Consistent** Meta consistently identified as sender
Recipient	"relief efforts" ❌ Vague description	"relief efforts" ❌ Vague description	"relief organizations" ⚠ More precise but limited	**Slight improvement** From vague to somewhat more precise
Subject	Meta users ❌ Implicit, not stated	Meta users ❌ Implicit, not stated	Meta users ❌ Implicit, not stated	**Consistently inadequate** Never explicitly identified across all versions
Information Type	"information we have" "migration patterns" ❌ Limited examples	"information we have" "migration patterns" ❌ Limited examples	"information" "migration patterns" ❌ Limited examples	**No improvement** Remains highly abstract with no expansion of data types
Transmission Principle	"research and innovation" ❌ Technology-neutral	"research and innovation" ❌ Technology-neutral	"automatic processing" "artificial intelligence" "machine learning" ✅ Technology-specific	**Significant improvement** From technology-neutral to explicit AI terminology

Regulatory Compliance Assessment of Meta's Privacy Policies (2018-2024)

Methods

This research conducts a systematic longitudinal analysis of how AI-based information handling practices are disclosed and evolve in platform privacy policies, using Meta as a strategic case study.

Three versions of Meta's privacy policy representing key evolutionary stages: September 2018: Pre-AI explicit usage era (post-GDPR implementation); January 2022: Early AI integration period; June 2024: Advanced AI adoption under expanded regulatory frameworks (GDPR and EU AI Act). By examining these significant policy versions across a six-year period marked by major regulatory and technological shifts, we trace the evolution of AI data practice disclosures. We use the CI-based method (Shvartzshnaider et al., 2019) to:

A) Systematically annotate CI parameters across three policy versions
B) Establish mapping relationships between CI parameters and legal requirements
C) Assess changes in privacy policy compliance over time (Bhatia et al., 2016; Harkous et al., 2018)

"Research and innovate for social good. We [sender] use the **information we have [attribution]** (including from research partners we collaborate with) to conduct and support **research and innovation on topics of general social welfare, technological advancement, public interest, health and well-being [transmission principle]**. For example, we [sender] analyze **information we have about migration patterns [attribution]** during crises to aid **relief efforts [recipient]**."

Example: CI annotation of a privacy policy statement

Analysis

Initial findings

A) Meta's privacy policy language evolved from technology-neutral terminology in 2018 ("technological advancement"), to indirect references to automated systems in 2022, to explicit acknowledgment of "artificial intelligence and machine learning" in 2024, reflecting strategic transparency adaptation.
B) While sender identification remained consistent and transmission principles became more explicit over time, information types stayed vague and subjects (users) remained implicit across all versions, creating structural information asymmetries.
C) Minimal substantive improvement in compliance across versions, despite significant regulatory developments (GDPR implementation and EU AI Act).
D) Reveal a critical pattern where the 2024 policy acknowledges AI usage (transmission principle) without corresponding enhancement of user control mechanisms, creating a disclosure-control gap that undermines contextual integrity.

Summary: We assess compliance by mapping CI parameters to regulatory requirements. Using keyword matching and contextual analysis, we link the principle of transfer to transparency requirements, the type of information to the purpose limitation, and the subject processing to the rights of the data subject. Based on clear disclosure of the purposes of processing, specificity of the categories of data used, clear explanations of automated decision-making, and documented risk mitigation measures, we evaluate each version of the Policy using a three-level scoring scale (non-compliant, partially compliant, fully compliant).

Next steps: 1) We will document Meta's transition from a data collector to a processor-controller hybrid by annotating the privacy policy with the CI parameter. 2) We will assess specific compliance deficiencies in the Privacy Policy in conjunction with the AI Risk Assessment Framework and Automated Decision Interpretation required by the EU AI Act.

References

Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. Big Data & Society, 8(1), 20539517211017308.
Bhatia, J., et al. (2016). A theory of vagueness and privacy risk perception.
Cox, A. M., & Tam, W. W. T. (2018). A critical analysis of lifecycle models of the research process and research data management. Aslib Journal of Information Management, 70(2), 142–157.
European Data Protection Board. (2018). Guidelines on transparency under Regulation 2016/679 [WP260 rev.01]. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/transparency_en
European Parliament. (2023). EU AI Act: first regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.
Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 531-548).
International Association of Privacy Professionals. (2024). 2024 global legislative predictions. https://iapp.org/resources/article/global-legislative-predictions/
Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79, 119.
Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, 140(4), 32–48.
Paramesha, M., Rane, N. L., & Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. Partners Universal Multidisciplinary Research Journal, 1(2), 110-133.
Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN computer science, 2(3), 160.
Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2018). Analyzing privacy policies using contextual integrity annotations. arXiv preprint, arXiv:1809.02236.
Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis. In Proceedings of the AAAI Conference on Human Computation and Crowdsourcing (Vol. 7, pp. 162–170).

Acknowledgements

Thanks to supervisors Yan Shvartzshniadiser and Kean Birch for supporting this work.