AI-Driven Privacy Transparency for Mobile Health Applications

Ayush Patel, Dr Richard Paige

Department of Computing and Software, McMaster University, Hamilton, Canada | McMaster Center for Software Certification (McSCert)

Introduction

- Mobile health apps raise significant privacy and security challenges, affecting user trust
- There is a disconnect between users and complex privacy policies that require a college-level education to understand and hidden deep within apps [1].
- Most users "consent" to data collection practices by simply clicking "agree" without reading the full policy, leading to a lack of transparency.
- Large Language Models (LLMs), offer a promising way to bridge this gap by providing real-time, user-friendly explanations. These explanations must be:
  - **Logically Consistent** with regulations (PIPEDA) and the app's privacy policy.
  - **Readable** to the average user (approx. 8th grade)
  - **Concise** to fit on mobile screens

Objectives

- **Develop an AI-driven system** that detects and explains privacy violations in real-time
- **Create an interface** with embedded UI elements that provide real-time, contextual privacy awareness directly on app screens
- **Measure the relationship** between explanation length, readability, and logical consistency to optimize AI-generated responses for mobile use.

Prototype Development

- A proof-of-concept sleep tracking app was built to demonstrate real-world feasibility of the privacy transparency tool.
- The app uses Google's Gemini LLM to analyze data collection events, assess privacy risks, and generate explanations based on PIPEDA principles, privacy policies, and user consent.
- **Tooltip UI:** Privacy icons next to specific data types reveal contextual information on click. (Figure 1 - left)
- **Privacy Page UI:** A single icon on each screen expands to a comprehensive privacy page for all collected data. (Figure 1 - right)

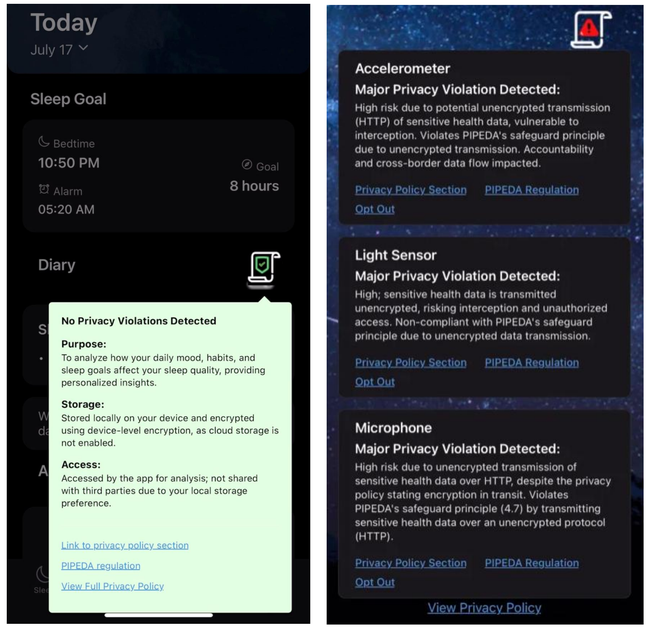

Figure 1: Tooltip UI showing no privacy concerns (left), Full page converted into privacy UI with major concerns (right)

Consistency vs Readability vs Length Experiment

- **Methodology**
  - **Goal:** Determine relationship between logical consistency, readability, and length to optimize the AI explanations
  - Readability assessed using Flesch-Kincaid Grade Level and SUBTLEX-US Word Frequency (on a zipf scale of 1-7) [2].
  - Consistency measured using a Natural Language Inference model (DeBERTa) against PIPEDA and policy text [3].
- **Results**
  - Avg NLI score = **0.749,** avg FK grade = **9.20**, average word freq = **5.03**

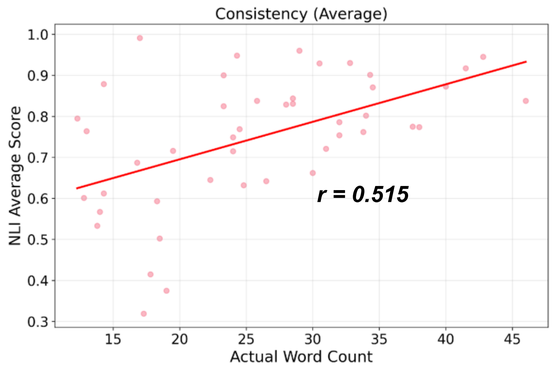

Figure 2: Moderate positive correlation between length and NLI scores

- **No significant correlation** between length and FK grade ***(r = -0.007)***
- **Weak positive correlation** between length and word freq ***(r = 0.365)***

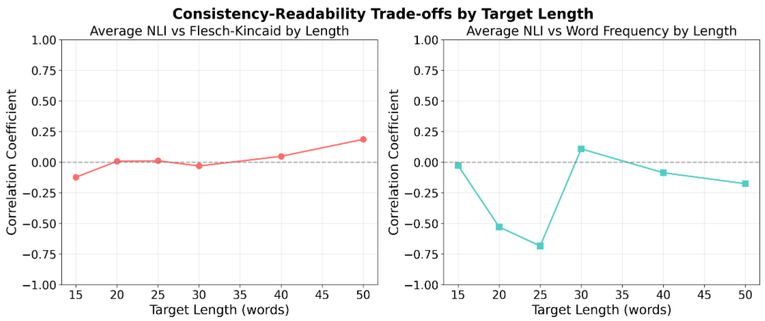

Figure 3: NLI vs Flesch-Kincaid and NLI vs word frequency correlations by length

Conclusion

- The prototype demonstrates the technical feasibility of using an AI-driven tool to provide real-time privacy explanations
- The relationships between explanation length, readability, and consistency are complex and **inconclusive**.
- The study highlights key challenges: the lack of a single "ideal" response length and the difficulties of reliably determining the quality of AI-generated explanations

Future Work

- Conduct comprehensive user studies to validate whether the AI explanations and embedded UI elements truly improve user understanding and privacy awareness.
- Use enhanced readability and logical consistency metrics

References

[1] A. Adhikari, "Natural Language Processing of Privacy Policies: A Survey," arXiv.org, Jan. 17, 2025. [Online]. Available: https://arxiv.org/html/2501.10319v1. [Accessed: Jun. 02, 2025].

[2] W. J. B. van Heuven, P. Mandera, E. Keuleers, and M. Brysbaert, "Subtlex-UK: A New and Improved Word Frequency Database for British English," Quart. J. Exp. Psych., vol. 67, no. 6, pp. 1176–1190, Jun. 2014, doi: 10.1080/17470218.2013.850521.

[3] M. Laurer, "MoritzLaurer/DeBERTa-v3-large-mnli-fever-anli-ling-wanli · Hugging Face," huggingface.co, Apr. 05, 2023. [Online]. Available: https://huggingface.co/MoritzLaurer/DeBERTa-v3-large-mnli-fever-anli-ling-wanli.

Ayush Patel
Undergraduate Software Engineering III
McMaster University, Department of Computing and Software, Faculty of Engineering
Email: patea237@mcmaster.ca

BRIGHTER WORLD