# RISHABH KHANDELWAL

https://shrishabh.github.io

## Education

**University of Wisconsin – Madison**
Doctoral Student - Computer Science — *Expected Dec'23* (Available to Work: Oct 1, 2023)
MS - Computer Science — *2021*
MA Physics — *2019*

**Indian Institute of Technology - Bombay**
Bachelor and Master of Technology in Engineering Physics — *2016*

## Research Interests

Large Language Models, Information Retrieval, Recommendation Systems, Transformers, Applications of Generative AI, Usable Privacy

## Work Experience

**Research Intern, Systems AI Lab, Telefonica Research** (Aug 2023 - Present)
*Summary:* Conducting experiments to evaluate 'Federated Learning as a Service' (FLaaS) against fairness and poisoning attacks, using both differential privacy and hierarchical federated learning.

**Research Intern, Aether Privacy Group, Microsoft Research** (June 2022 - Sept 2022)
*Summary:* Conducted a qualitative study to identify the challenges and needs of the participants in the privacy review process for features/products with Machine Learning components.

**Student Researcher, Applied Privacy Research, Google Inc.** (Sept 2021 - Oct 2021)
*Summary:* Worked on the privacy review classification problem using **Large Language Models (LLMs)** for the automated privacy review analysis project. The work was submitted and accepted for publication in IEEE SP, 2022.

**Research Intern, Applied Privacy Research, Google Inc.** (May 2021 - August 2021)
*Summary:* Built an automated pipeline leveraging **LLMs** to extract privacy issues from the app reviews. The system is currently being used in developer studies to test production readiness.

## Selected Publications

**R. Khandelwal**, A. Nayak, P. Chung, and K. Fawaz. **Unpacking Privacy Labels: Measurement and Developer Perspective on Google's DSS** USENIX Security, 2024 (*Rev.*).

**R. Khandelwal**, A. Nayak, H. Harkous, and K. Fawaz. **CookieEnforcer: Automated Cookie Notice Analysis and Enforcement.** USENIX Security, 2023 (Accept. Rate: 15%)

H. Harkous, S. Pedinnti, **R. Khandelwal**, A. Srivastava, and N. Taft. **Hark: A Deep Learning System for Navigating Privacy Feedback at Scale.** IEEE SP, 2022 *(Accept. Rate: 13.7%)*

**R. Khandelwal**, T. Linden, K. Fawaz and H. Harkous. **PriSEC: A Privacy Settings Enforcement Controller.** USENIX Security, 2021 *(Accept. Rate: 18.6%)*

**R. Khandelwal**, A. Nayak, Y. Yao and K. Fawaz. **Surfacing Privacy Settings Using Semantic Matching.** PrivateNLP@EMNLP 2020

T. Linden, **R. Khandelwal**, K. Fawaz and H. Harkous. **The Privacy Policy Landscape After the GDPR** 20th Privacy Enhancing Technologies Symposium, 2020 *(Accept. Rate: 22%)*

**R. Khandelwal**, M.Y. Lu and A. Karle on behalf of the ARA Collaboration. **Optimization of Radio Detectors in Ice**. 35th International Cosmic Ray Conference, 2017

C.A. Arguelles, K. Farrag, T. Katori, **R. Khandelwal**, S. Mandalia and J. Salvado. **Probe Of Sterile Neutrinos Using Astrophysical Neutrino Flavor**, JCAP

*A Complete list of publications can be found here: Link

## Under Submission

**R. Khandelwal**, A. Nayak, and K. Fawaz. **Exposing and Addressing Security Vulnerabilities in Text Input Fields.** The Web Conference 2024.

**R. Khandelwal**, P. Chung, A. Nayak, and K. Fawaz. **Taxonomies for Automated Privacy Policy Analysis and Privacy Label Generation.** WPES, CCS 2023.

**R. Khandelwal**, A. Nayak, P. Chung, and K. Fawaz. **Comparing Privacy Labels of Applications in Android and iOS.** WPES, CCS 2023.

## Ongoing Work

**LLM powered Consistency Framework for Privacy Documents**
*Mentors: Prof. Kassem Fawaz*
Developing a framework that uses LLM agents in conjunction with LangChain to assess the consistency of privacy documents. These LLM agents analyze the privacy documents to ensure they align with privacy labels, regulations, and maintain internal consistency.

**Multi-modal analysis of webpages for privacy solutions**
*Mentors: Prof. Kassem Fawaz*
Building a framework to analyze webpages and develop automated solutions for privacy-related tasks. By leveraging both visual and textual features of the webpage, our framework can automate privacy tasks, including adjusting privacy settings and deactivating non-essential cookies.

**Applications of LLMs in Clean Energy Sector**
Assisting in the development of a framework that uses Large Language Models to automatically scrape and analyze ESG reports from companies. The data extracted serves to establish benchmarks, compare practices among companies, and conduct compliance analysis.

**AI Privacy in Privacy Reviews: From Theory to Practice**
*Mentors: Dr. Kim Laine, Dr. Boris Koepf, Dr. Mihaela Vorvoreanu*
**Research Internship - Microsoft Research**
Conducted qualitative study to identify the challenges that the participants face and the tools to optimize the privacy review process.
**Impact:** The results are being used to streamline the privacy review process, as well as inform future projects in the Aether Privacy Working group.

**AI-Powered Diagnostics and Generation of Android Permission Rationales**
*Mentors: Prof. Kassem Fawaz, Dr. Hamza Harkous*
Assessing data collection consistency by comparing app privacy policies with purposes stated in rationales using Large Language Models, and employed these models to evaluate rationale specificity and readability.

## Talks and Posters

**Hark: Deep Learning System for Navigating Feedback** CSAW, November 2022 (Poster)

**CookieEnforcer: Automated Cookie Notice Analysis and Enforcement.** MSR, July 2022.

**PriSEC: Privacy Setting Enforcement Controller** Google, June 2021 (Lightning Talk)

## Research In News

Our work on **Automating Cookie Notice Analysis and Enforcement** was covered by The Gradient (Link), Unite.AI (Link) and Techradar (Link)

Our work on **Exposing and Addressing Security Vulnerabilities in Text Input Fields** was covered by BleepingComputer (Link), Malwarebytes (Link), TechRadar (Link), The Sun (Link), Mirror UK (Link) and India Times (Link).

## Technical Skills

**Languages:** Python, Java, C++, R, Matlab

**Frameworks:** PyTorch, Tensorflow, JAX, Flax

## Patents

US Patent App 63/365,071, "Deep Learning System for Navigating Feedback", H. Harkous, S. Pedinnti, **R. Khandelwal**, A. Srivastava, and N. Taft, May 20, 2022 (Pending)

## Service

External Reviewer - ACM Trasactions on Privacy and Security (2022),
Sub-reviewer - USENIX (2021, 2022), IEEE S&P (2021, 2022, 2023), PETs (2021, 2022)

## Scholastic Achievements

- Awarded Student Research Grant by the Graduate School at UW Madison, 2023.
- Finalist in CSAW - Applied Privacy Research competition, 2022
- Secured the first position in CS Research Symposium, 2022 (UW Madison).
- Finalist in Qualcomm Innovation Fellowship, 2021
- Awarded the **Piore Award** by Department of Physics, UW Madison for performance in Quals