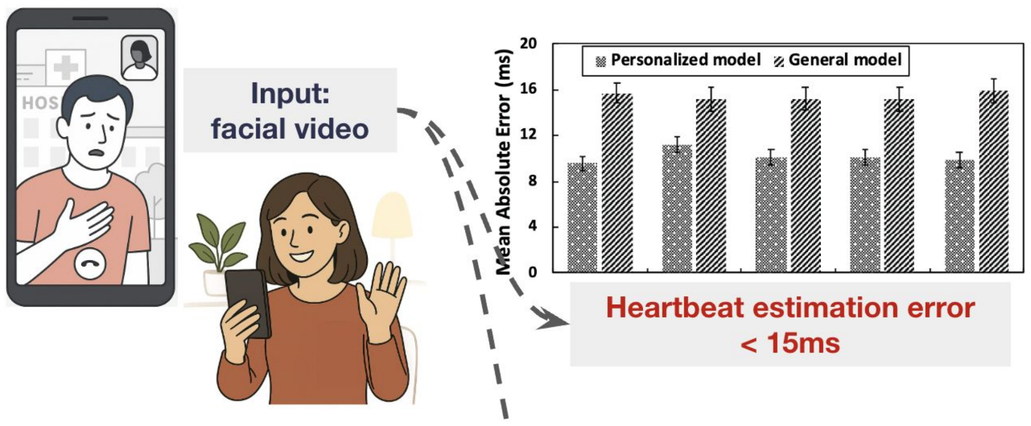
Revealing the Unseen: User-Centered OS-Level Controls for Inference-Aware Privacy

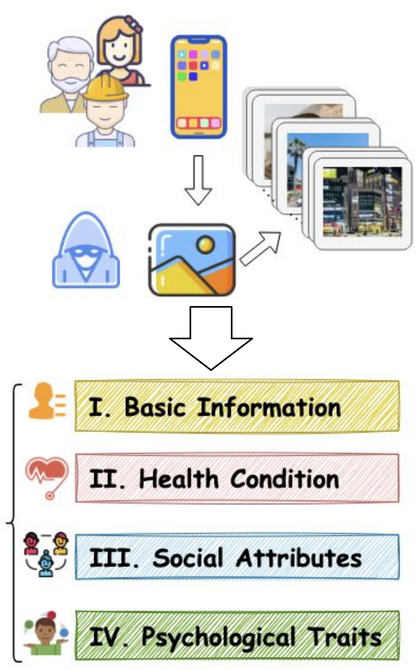
Sieun Park, Youngki Lee
Seoul National University

Deep Models Infer More Than You Expect — From Less Than You Think



		HRV features								
Statistic	Source	RMSSD	SDNN	MRRI	NN50	PNN50	SD1	SD2	LFnu	HFnu
Mean	ECG	112.20	88.51	751.00	9.88	13.46	80.36	95.39	25.97	74.10
Mean	VitaMon	114.51	89.47	750.15	16.46	23.30	80.55	95.77	30.66	68.81
Standard Deviation	ECG	69.94	44.82	68.52	9.33	12.46	49.66	42.79	30.54	30.54
Standard Deviation	VitaMon	61.29	41.49	68.38	9.55					
Correlation Coefficient		0.9879	0.9836	0.9855	0.7948	0.7394	0.9861	0.9830	0.8134	0.8139

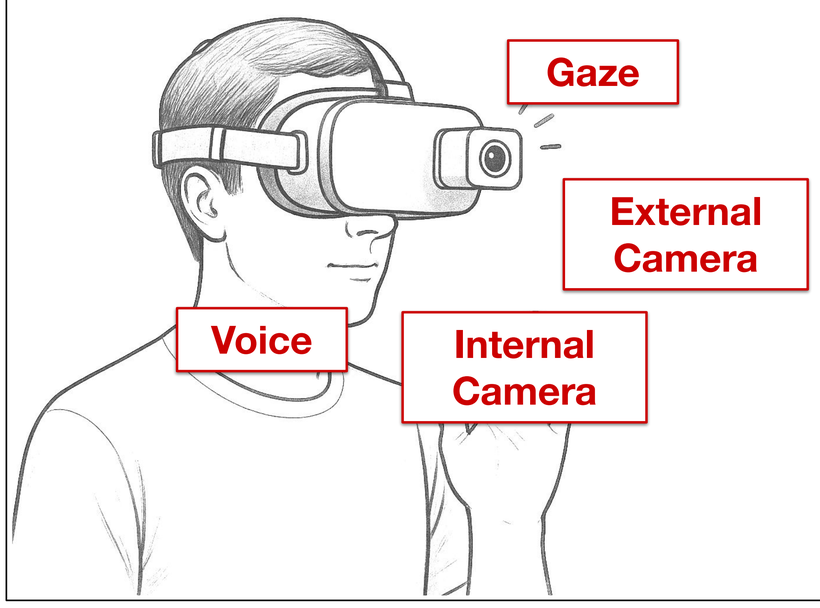
HRV feature high correlation

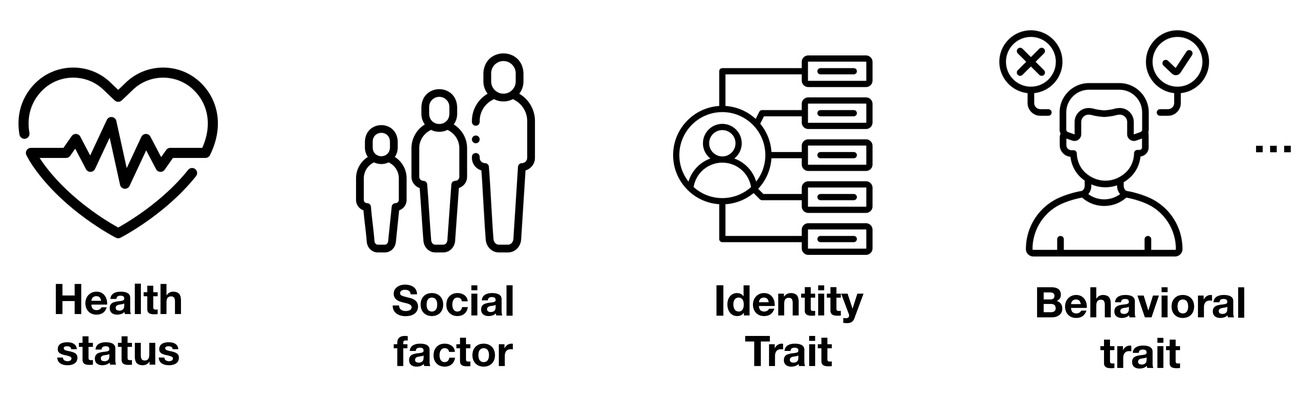


Deep learning model infers user's heart rate from a few-second facial video

LLM predicts the exact location of a user from a single image

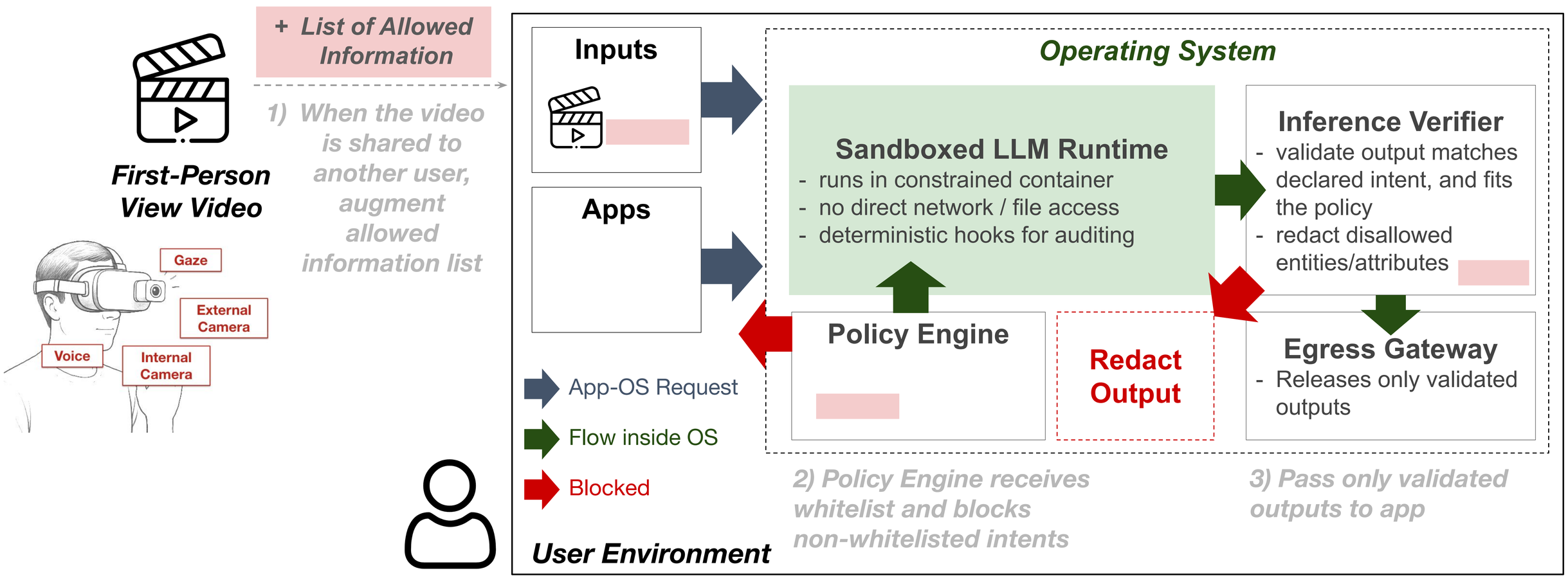
LLM predicts personal portraits





In input-rich telepresence, richer sharing means greater presence — and greater privacy threat.

Solution: OS-Level Whitelist-based Control for Inference Attacks



Discussion Points

- Transparency of Inference
  → How can we make hidden inference flows visible without overwhelming users?
- User Agency and Control
  → How can we give users fine-grained control in simple, unobtrusive ways?
- Balancing Utility and Privacy
  → How can interactions negotiate between usefulness and protection?

Contact

Sieun Park
Seoul National University
Human-Centered Computer Systems Lab
Feel free to reach out!