1 Speaker Notes

1.1 SLIDE 1: Title Slide

Excellencies, ladies, and gentlemen. My name is Monireach, a Master's research student. Today I'll present our design study on privacy governance-driven AI architecture for elderly safety monitoring in Cambodia. This research demonstrates how privacy governance principles can inform architectural decisions from the beginning, rather than being retrofitted after deployment. The work aligns with this conference's theme of governing emerging intelligent technologies, as it examines the combination of privacy governance, edge computing, and accessibility in resource-constrained healthcare contexts.

Transition: Let me start by framing the challenge we're addressing.

1.2 SLIDE 2: The Challenge - Elderly Safety Dilemma

Southeast Asia is facing a rapidly aging population, according to WHO SEARO, elderly population is estimated to increase from 12.2% in 2024 to nearly 23% by 2050. Falls are the leading cause of injury-related deaths among elderly, with 684,000 annual fatalities globally, and 60% concentrated in the Western Pacific and Southeast Asia regions. In Cambodia specifically, we're projecting 1.8 million elderly by 2030.

Current monitoring solutions force families to choose between privacy and effectiveness. Cloud-based cameras transmit video to third-party servers, creating facial recognition and re-identification risks. The Kami Fall Detect Camera, for example, requires continuous cloud connectivity and costs $1,719 over three years due to mandatory subscriptions. Wearables offer better privacy but come with particular challenges—elderly users must remember to wear devices consistently and maintain charging, which is particularly difficult at nighttime.

We're targeting middle-income Cambodian households—families earning 870 to 1622 US Dollars per month. For them, a $45 monthly cloud subscription means paying 5.2% of their income every month, indefinitely. That's not sustainable. But these families still need reliable safety monitoring for their aging parents at home.

Transition: This brings us to our research question.

1.3 SLIDE 3: What We're Investigating

Let me explain what we're investigating in plain terms first.

The core problem: elderly monitoring cameras today force families to choose. Either send video footage to cloud companies—which creates privacy risks from facial recognition and re-identification—or use wearables that elderly people forget to wear or charge, especially at night.

We're asking: can we design a system that protects privacy by keeping all data at home, works 24/7 without requiring wearables, and costs less than cloud alternatives?

In academic framing, our research question is: how can privacy governance principles—the rules about handling personal data—inform the architectural design of AI-based elderly monitoring systems in resource-constrained contexts like developing countries?

This is a design study. We're demonstrating how governance principles can drive architecture choices. We validate three things: whether affordable infrared cameras work with AI pose detection, whether edge-based systems cost less than cloud alternatives, and whether our architecture eliminates facial data collection by design.

We're not validating fall detection accuracy on benchmark datasets—that's future work. We're not deploying in real homes yet. We're showing that privacy-first edge architecture is technically and economically viable.

Transition: So what specifically are we exploring?

1.4 SLIDE 4: Three Design Propositions

We explore three design propositions.

First: can privacy governance translate directly into technical architecture? If privacy rules say "must protect privacy," can we translate that into specific choices—edge computing, pose-only data storage, and deleting video frames immediately after processing?

Second: does privacy-first design yield cost reduction? Our hypothesis is that eliminating cloud infrastructure for privacy reasons also eliminates expensive subscription fees, creating an economic benefit beyond privacy protection.

Third: can body pose data alone enable safety monitoring? Can we detect falls using just skeletal keypoints—17 body joint coordinates—without storing actual video footage?

Our testing approach validates feasibility through NIR camera compatibility testing and cost-effectiveness analysis. We're showing this architecture is viable before investing in full system deployment.

Transition: Let me show you the architecture we designed based on these propositions.

1.5 SLIDE 5: Privacy Governance Architecture

Our architecture translates privacy requirements into three concrete design choices.

First, edge-first processing. What does this mean? All the computing happens on a small box in your home—specifically, an NVIDIA GPU called Jetson Orin Nano. Nothing gets sent to the internet. Zero. The video never touches a cloud server, never crosses a network. Your elderly parent's health data physically cannot leave the house. That's what we mean by data sovereignty.

Second, pose-only storage. The system watches the video and extracts just 17 body joint coordinates—like connect-the-dots for a skeleton. Where are the shoulders? Where are the hips? That's all we keep. We deliberately exclude face landmarks. Here's the key point: you cannot reverse-engineer a person's face from skeletal coordinates. It's not just that we promise not to look at faces—the facial information literally doesn't exist in our data. The architecture makes facial recognition impossible, not just prohibited.

Third, immediate frame disposal. The camera captures video frames. Our software processes each frame in real-time to extract those 17 body points. Then the frame gets deleted. Immediately. We don't store video footage at all. No video means no way to re-identify the person later—you can't go back and look at someone's face because the video is already gone.

This approach is called privacy by design. The difference from typical systems: we're building privacy into the architecture from day one, not adding privacy controls after the system is already deployed. The system enforces privacy through what it physically can and cannot do, not through policies that someone might

violate later.

Transition: Let me briefly outline the technical implementation.

1.6 SLIDE 6: Technical Approach Overview

Let me give you a quick overview of the technical setup—don't worry, I'll keep this simple.

Hardware: Four cameras positioned around the room, 90 degrees apart, so they cover the entire space—360-degree coverage. These are ordinary security cameras, but they have infrared night vision. That means they work in complete darkness, 24/7. No need to keep lights on at night. Total cost for the whole system: $672 one-time payment. No monthly fees.

Software: Three steps. First, the system detects where the person is in the video frame—just finds the person. Second, it extracts the body pose—those 17 skeleton points we talked about earlier. Third, our privacy layer kicks in—deletes the video frame immediately, keeps only the pose coordinates. That's it.

This is the technical architecture we validated. I'm happy to discuss implementation details during Q&A if anyone's interested in the specific AI models or camera specifications.

Transition: Now, what exactly did we validate in this study?

1.7 SLIDE 7: Results - NIR Camera Compatibility

Let's look at our first validation result: does AI pose detection actually work on infrared night vision cameras?

Testing approach: We collected 20 commercial security camera videos from different manufacturers—Hikvision, EZviz, dome cameras, bullet cameras—filmed in different environments, both indoor and outdoor. These are real infrared videos at 1080p and 4K resolution. We wanted to see if our software works across different camera types, not just one specific model.

The results: Our system detected body poses in 91.3% of video frames. That's detecting about 30 out of 33 body points per frame. The confidence score averaged 0.868—in simple terms, the system is quite

certain about what it's detecting. False negatives—situations where a person is there but the system fails to detect their pose—happened 12.3% of the time. Processing speed was about 20 frames per second.

Why this matters: The AI model we're using—MediaPipe—was originally trained on regular color images in daylight. We're testing it on infrared footage in complete darkness. And it works. This confirms you can monitor elderly people 24/7 using cheap security cameras without needing facial recognition technology. You get privacy by design while maintaining monitoring capability.

Very little research has actually tested whether pose detection works on the specific infrared wavelength used in affordable security cameras. We're showing it does.

Transition: Now let me show you the cost-effectiveness analysis.

1.8 SLIDE 8: Results - Cost-Effectiveness Analysis

Now let's talk about cost. Does privacy-first design actually save money?

Our system costs $672 upfront. That's $252 for four cameras, $250 for the edge processor, and $170 for accessories like storage and cables. One-time payment. No monthly fees. Ever.

Compare that to cloud alternatives. We looked at the Kami Fall Detect Camera—it's a camera-based elderly fall detection system, similar to what we're building. The hardware costs $99, which sounds cheap. But there's a mandatory subscription: $45 every month. Do the math over three years: $99 hardware plus $1,620 in subscription fees equals $1,719 total.

The savings: 61% cost reduction. Our system saves families $1,047 over three years. The breakeven point? Month 13 of year two. After that, every month the cloud alternative keeps charging $45 while our system costs nothing.

Who can afford this? We're targeting middle-income Cambodian households—families earning 870 to 1622 US Dollars per month. That's the fourth and fifth income quintiles. For these families, a $45 monthly subscription means paying 5.2% of their income every single month, indefinitely. Our $672 one-time cost is equivalent to about half a month's income. Families can save up for it, or pool money together.

Market reach: We estimate this could reach 12 to 18% of Cambodia's elderly population—those living

in urban middle-income households, totalling 252,000 to 378,000 people by 2030.

Here's the key point: we eliminated cloud infrastructure for privacy reasons. The cost savings is a side benefit. Privacy governance actually enables affordability.

Transition: Let me explain a key design trade-off we encountered.

1.9 SLIDE 9: Design Trade-offs - Safety-Critical Priority

After designing our privacy-first architecture, we needed to validate it actually works technically. So we tested two different approaches to see which performs better.

Baseline: Just run pose detection on the whole video frame. Simple.

Integrated: First detect where the person is, crop that area, then run pose detection on just that cropped region. More complex.

The trade-off: The integrated approach is more accurate—it detects 5.7% more keypoints and has 22% better coverage. But it's 2.3 times slower. The baseline processes 47 frames per second. The integrated version? Only 20 frames per second.

Which did we choose? The integrated pipeline. Why? Because accuracy matters more than speed in this context. If the system misses a fall—if grandma falls and the camera doesn't detect it—that could be fatal. Speed is nice to have. Accuracy is life-or-death.

And here's the important part: even the slower integrated pipeline runs at 20 frames per second. Our target for real-time monitoring is 15 frames per second. We're still well above that threshold.

This shows a governance principle at work: technical metrics don't exist in a vacuum. You have to evaluate performance against consequences. In safety-critical healthcare applications, we optimize for accuracy first, speed second.

Transition: These technical results lead to broader governance implications.

1.10 SLIDE 10: What This Means for Governance

Let me connect the dots on what these results mean for governance.

First key finding: Privacy by design actually works. We proved you can build a privacy-first system that performs well—91.3% detection rate on infrared cameras. You don't have to choose between privacy and performance.

Second: Privacy governance creates unexpected economic benefits. We eliminated cloud infrastructure for privacy reasons, which also eliminated subscription costs. This makes healthcare AI affordable for middle-income markets in developing countries. Privacy governance enables accessibility governance.

Third: Context-specific design matters. We designed for Cambodia's economic constraints—targeting families earning 870 to 1,622 US Dollars per month. This approach scales to other developing countries with similar resource constraints.

The bottom line: governance principles can drive technical architecture from inception, not as afterthoughts. We're showing how to do privacy-first AI design in practice.

Transition: Let me ground this in the Cambodia context.

1.11 SLIDE 11: Regional Impact - Cambodia Case Study

Let me show you why the Cambodia context matters.

Who are we designing for? Middle-income Cambodian households—families earning 870 to 1,622 US Dollars per month. That's the fourth and fifth income quintiles according to Cambodia's Socio-Economic Survey. These families face a real problem: cloud subscriptions cost $45 monthly, which is 5.2% of their income every single month. That's not sustainable long-term.

Our edge-based system costs $672 one-time. That's equivalent to about half a month to a full month of income—a significant upfront cost, yes, but families can save for it or pool resources. And then? Zero recurring fees. This model could reach 252,000 to 378,000 Cambodian elderly by 2030—that's 12 to 18% of the elderly population living in urban middle-income households.

Why does Cambodia matter beyond Cambodia? Cambodia serves as a proof-of-concept for resource-

constrained contexts. We designed for specific constraints: aging populations, middle-income markets, privacy concerns without strong enforcement, cost sensitivity, and bandwidth limitations.

If privacy-first architecture works here—technically and economically—it can scale to other developing countries facing similar constraints.

Transition: Let me address limitations and future directions.

1.12 SLIDE 12: Limitations & Future Directions

Let me be honest about the limitations.

First limitation: Testing environment. We tested on commercial security camera footage, not actual elderly people. Elderly individuals may move differently—different gait patterns, body proportions. Our validation shows the technology works, but we need to test with the actual target population.

Second: Hardware deployment. We measured performance on standard laptop hardware, not the actual Jetson Orin Nano edge device we're proposing. We got 20 frames per second on the laptop. The Jetson might perform differently—could be faster, could be slower. We need to validate on the actual hardware.

Third: Market accessibility. Our $672 system targets middle-income urban households. What about low-income families? What about rural areas? Those populations need different deployment models—maybe government subsidies, maybe community-based financing. We haven't solved accessibility for everyone, just for the middle-income segment.

What's next? Three immediate priorities. First, test fall detection accuracy on benchmark datasets—actually measure how well the system detects falls. Second, deploy on the Jetson hardware and validate real-world performance. Third, collect our own dataset with Cambodian elderly participants—real people in real homes.

Longer-term, we need user acceptance studies. Will elderly people and their caregivers actually use this system? That's the ultimate test—not just technical performance, but real-world adoption.

Transition: Let me conclude with key takeaways.

1.13 SLIDE 13: Conclusion - Key Takeaways

Let me wrap up with four key takeaways.

First: Privacy governance can drive technical design from day one. We're not adding privacy controls after building the system—we're building privacy into the architecture itself. Edge processing, pose-only storage, immediate frame disposal. The system physically cannot violate privacy because the architecture prevents it.

Second: Privacy-first design doesn't sacrifice performance. We validated 91.3% keypoint detection on infrared footage—the system works in complete darkness, 24/7. And we demonstrated 61% cost savings compared to cloud alternatives. $672 one-time versus $1,719 over three years.

Third: Privacy creates unexpected economic benefits. We eliminated cloud infrastructure for privacy reasons, which also eliminated subscription costs. This makes the technology affordable for middle-income markets—reaching 252,000 to 378,000 Cambodian elderly, 12 to 18% of the population.

Fourth: Context-specific design matters. We designed for Cambodia's economic constraints—targeting families earning 870 to 1,622 US Dollars per month. This isn't just about Cambodia. It's a proof-of-concept showing privacy-first architecture can work in resource-constrained settings.

What does this mean practically? Three groups should care about this work. Researchers: validate infrared camera compatibility before you deploy—we found performance varies significantly by camera type. Policymakers: recognize that privacy-first architecture can actually expand accessibility in middle-income markets through cost reduction. Practitioners building elderly care systems: consider zero-subscription models to reduce ongoing cost barriers in developing countries.

Thank you for your attention. I'm happy to take questions.