Week 2: Skill Selection & Analysis Preparation

Introduction

This report examines the privacy and security implications of ten popular Alexa skills, ranging from low-risk entertainment apps to high-risk financial and health-related tools. The goal is to identify what each skill collects, where that data goes, and whether it aligns with what the company claims in its privacy policy. By analyzing permissions, data flows, and actual behavior, we can determine whether these skills are trustworthy or pose potential risks. This project highlights the importance of transparency, responsible app design, and user awareness when interacting with voice-based smart technologies.

Deliverable

A clear, easy-to-read list of chosen Alexa skills and what we will check for each one.

1. Selected Alexa Skills

1. Amazon Shopping – Handles orders and payment details (we will look at what shopping data it can access, like your address, order history, and saved cards).
2. Philips Hue – Controls your smart lights (we will note what device info and network access it needs, like Wi-Fi or other smart devices in your house).
3. Uber – Books rides with your location (we will check how it uses your real-time location and whether it stores your ride history).
4. Fitbit – Tracks your health stats (we will see which sensitive health metrics it collects like heart rate, sleep, steps, and if it follows privacy laws like HIPAA).
5. Capital One – Shows your account balances (we will verify if it securely handles banking login, balances, and transaction data).
6. Jeopardy! – Plays a trivia game (we will confirm that it uses minimal or no personal info and doesn't collect more than needed).
7. Order Pizza – Places food orders (we will inspect how it handles your delivery address, contact info, and payment data).
8. Ask My Buddy – Sends alerts in emergencies (we will review how it accesses and uses your location and emergency contact info).
9. Sleep Sounds – Plays relaxation sounds (we will check if it collects logs or usage data and ensure it doesn’t ask for unnecessary access).
10. Tinder – Matches with others (we will analyze how it handles profile data, photos, preferences, and any voice or mic access).

2. What We Will Check for Each Skill

- Permissions: What data or device controls the skill asks for. [Example: asking for your location, camera, or contact list]

- Privacy Policy: What the company says they will do with your data, and whether they actually do it.

- Data Flow: Where your data goes, what servers, third-party services, or cloud providers receive it.

- User Steps: Which voice commands or actions trigger data collection. [Example: does just opening the skill send info, or only when you use a certain command?]

- Revocation Behavior: What happens when you turn off or uninstall the skill — does your data get deleted, or is it kept?

3. Quick Analysis Checklist

- Compare requested permissions to what the skill actually uses. [Is it asking for more access than it needs?]
- Match privacy policy promises with what really happens in use. [Do they collect more than they say?]
- Identify all external servers or services involved in data transfer. [Does the data go to Amazon only, or also to third parties?]
- Check how long data is stored and where. [Is your info stored forever? Is it stored in another country?]
- Flag any sensitive data being collected (like GPS, health info, or banking).
- Detect any unencrypted network traffic. [If your data is sent without encryption, it's at risk.]
- Watch for unnecessary permissions. [For example, a game asking for your location or contacts without needing it.]
- Look for unexpected or hidden network calls. [Could be sending data silently to unknown servers.]
- Ensure logs don’t leak personal info. [Usage logs should not store names, addresses, or account numbers.]
- Verify error messages don’t expose sensitive data. [No passwords or internal system details should show if something crashes.]

4. Why This Matters

These checks help identify which Alexa skills are safe and which may be risky. Some are low-risk like games and sound apps, but others involve personal, financial, or health data. That makes them high-risk if not properly secured.

Most users just click “enable” without knowing what data they’re sharing or who it’s being shared with. This project exposes that gap and shows how to evaluate apps from a security and privacy perspective.

This is also important for legal and ethical reasons. Some skills may be breaking data privacy laws like GDPR or HIPAA without users knowing. Others might be asking for too many permissions or sending data to third parties for ads or profiling.

Even small or simple skills like smart lights or sound apps can be used as entry points into your network or devices. If the skill is poorly built, it can open up privacy risks.

By going through this analysis, we build real-world experience in cybersecurity, ethical tech design, and understanding how voice-based systems work behind the scenes.

This isn’t just Alexa, it's a model for how to investigate any smart device or app that collects user data.