Is Your Smart Home Spying? A Quick Checklist

Introduction

Smart home devices bring convenience, but they also raise important privacy questions. Are your smart speakers, cameras, and other gadgets listening in or watching more than you realize? This checklist will help you quickly assess and improve the privacy of your smart home, without needing a tech degree. Let's make your smart home safe and secure!

Section 1: Smart Speakers (Amazon Echo, Google Home, Apple HomePod, etc.)

These devices are designed to listen for your commands, but they can sometimes record more than you intend. Here's how to check:

Checklist Items:

- **Review Voice History:** Regularly check and delete your voice recordings. Most platforms allow you to review and delete recordings through their app or web portal.
    - Action: Go to [Device App/Web Portal] -> Privacy Settings -> Voice History.
- **Disable Voice Recording (if available):** Some devices allow you to disable continuous voice recording, only activating when a wake word is detected. Be aware this might affect functionality.
    - Action: Check device settings for options like "Delete recordings after X time" or "Don't save recordings."
- **Mute Microphone When Not in Use:** Use the physical mute button on your device when you don't want it listening. This is the most reliable way to ensure privacy.
    - Action: Locate the microphone mute button (often with a microphone icon and a line through it).
- **Manage Third-Party Skills/Apps:** Review permissions for any third-party skills or apps you've enabled. They might have access to more data than you realize.
    - Action: Go to [Device App/Web Portal] -> Skills/Apps -> Review Permissions.

- **Understand Data Usage:** Read the privacy policy for your smart speaker. Understand what data is collected and how it's used.
    - Action: Search online for "[Device Name] privacy policy."

Section 2: Smart Cameras & Doorbells (Ring, Arlo, Nest Cam, etc.)

Security cameras are great for peace of mind, but improper settings can expose your home to unintended viewers.

Checklist Items:

- **Set Activity Zones:** Define specific areas for motion detection to avoid recording public spaces unnecessarily.
    - Action: In camera app settings, find "Motion Zones" or "Activity Zones."
- **Review Sharing Settings:** Ensure your camera footage is not being shared with unintended individuals or third parties. Be cautious with family sharing options.
    - Action: In camera app settings, find "Sharing" or "User Access."
- **Enable Two-Factor Authentication (2FA):** Protect your camera account with 2FA to prevent unauthorized access.
    - Action: In account settings, enable 2FA.
- **Secure Wi-Fi Network:** Ensure your home Wi-Fi network is strong and secure (WPA2/WPA3 encryption, strong password).
    - Action: Check your router settings.
- **Physical Placement:** Consider where your cameras are pointed. Avoid pointing them into neighbors' windows or public areas if not necessary for security.
    - Action: Physically adjust camera angles.
- **Regularly Update Firmware:** Keep your camera's software up to date to patch security vulnerabilities.
    - Action: Check camera app for firmware updates.

Section 3: Smart TVs & Streaming Devices (Roku, Apple TV, Samsung Smart TV, etc.)

Modern TVs collect data on your viewing habits and can have microphones for voice control.

Checklist Items:

- **Disable "Smart Interactivity" / ACR (Automatic Content Recognition):** This feature allows your TV to identify what you're watching and send data back to the manufacturer or advertisers.
    - Action: Go to TV Settings -> Privacy/Smart Features -> Disable ACR or "Viewing Information Services."
- **Review App Permissions:** Check the permissions for apps installed on your smart TV or streaming device.
    - Action: Go to TV/Device Settings -> Apps -> Permissions.
- **Disable Voice Control Microphone (if not used):** If you don't use voice commands, disable the microphone on your TV or remote.
    - Action: Check TV settings or remote settings for microphone options.
- **Limit Ad Tracking:** Opt out of personalized ads if the option is available.
    - Action: Go to TV Settings -> Privacy/Advertising -> Limit Ad Tracking.
- **Use a VPN (Optional but Recommended):** A VPN can encrypt your internet traffic, adding an extra layer of privacy, especially when streaming.
    - Action: Install a VPN on your router or streaming device (if supported).

Section 4: Other Smart Devices (Thermostats, Light Bulbs, Appliances, etc.)

Even seemingly innocuous devices can collect data.

Checklist Items:

- **Review App Permissions:** Check what data the accompanying apps for these devices are collecting and what permissions they have.
    - Action: In your phone's app settings, review permissions for each smart device app.
- **Create a Separate IoT Network (Advanced):** For enhanced security, consider setting up a separate Wi-Fi network for your smart devices (IoT network) to isolate them from your main network.
    - Action: Consult your router's manual or ISP for guest network/VLAN setup.
- **Understand Data Sharing:** Be aware of whether your device data is shared with third-party partners.
    - Action: Read the privacy policy for each device/app.
- **Regularly Update Firmware:** Keep all smart devices updated to the latest firmware.
    - Action: Check device apps for update notifications.

Conclusion

Taking these steps can significantly improve your smart home's privacy posture. Remember, digital safety is an ongoing process. Regularly review your settings and stay informed about new privacy features and potential risks. Your peace of mind is worth it!