NO PREP

Smart Home AI

Thermostats, Doorbells, Security

Includes: Student reading, case study, differentiated questions, teacher key

Name: Period: Date:

Smart Home AI: Thermostats, Doorbells, Security

The Home That Learns Your Habits

The smart home was supposed to be the future. In 2010s tech advertisements, the vision was always the same: a homeowner arriving after a long day to find the lights already dimmed to their preferred level, the temperature set to exactly 68 degrees, and the security system automatically switching to 'home' mode. For millions of households, that vision has become partially real — and the AI behind it is more sophisticated than most people realize. Smart home devices are among the most intimate AI deployments in existence. Unlike a social media algorithm that studies your public scrolling behavior, a smart home AI lives inside your house. It knows when you wake up, when you go to bed, when you are away, what temperature you find

Name: Period: Date:

Smart Home AI: Thermostats, Doorbells, Security

The Home That Learns Your Habits

The smart home was supposed to be the future. In 2010s tech advertisements, the vision was always the same: a homeowner arriving after a long day to find the lights already dimmed to their preferred level, the temperature set to exactly 68 degrees, and the security system automatically switching to 'home' mode. For millions of households, that vision has become partially real, and the AI behind it is more sophisticated than most people realize. Smart home devices are among the most intimate AI deployments in existence. Unlike a social media algorithm that studies your public scrolling behavior, a smart home AI lives inside your house. It knows when you wake up, when you go to bed, when you are away, what temperature you find comfortable, who comes and goes, what you say out loud, and, with newer systems, what you look like. Understanding what these devices actually do with that information is not optional for anyone who uses them.

The Nest Thermostat: A Classic Case Study

The Nest Learning Thermostat, launched in 2011 and later acquired by Google in 2014, was the device that popularized the idea of the smart home. Its pitch was simple: stop manually adjusting your thermostat. Instead, let the device observe your patterns for about a week, learn your schedule, and automatically create a temperature program that matches your actual life rather than a generic preset. To do this, Nest uses a combination of behavioral learning and sensor data. It tracks every manual temperature adjustment you make and notes the time of day. It uses a built-in motion sensor to detect whether anyone is home, and it learns what temperatures correlate with your presence. After enough data collection, it builds a predictive model: at 6:45am on weekdays, someone wakes up; heat to 70. At 8:00am,

everyone leaves; drop to 60. At 5:30pm, expect someone home; begin heating. The model gets refined continuously as your schedule changes.

Ring Doorbells and the Video AI Layer

Ring, acquired by Amazon in 2018, operates at a different level of AI complexity. Ring cameras don't just record video: they use computer vision to analyze what they see in real time. Motion detection AI distinguishes between a moving branch, a car passing in the street, and a person approaching your door. Person detection specifically flags human movement and can send different alerts depending on whether it detects a person, a package, or a vehicle. Amazon has pushed Ring further into facial recognition territory. Ring's Neighbors app, a community sharing platform built into the Ring ecosystem, allows users to share footage of people the system flags as suspicious. This has generated significant controversy. Civil rights organizations have documented cases where Ring's Neighbors app was used to share footage of Black residents doing normal activities (walking, jogging, checking mail) with neighbors who found their presence suspicious. The AI flags the presence; the human bias determines what happens with that flag. Ring also has a documented history of sharing footage with law enforcement. Between 2020 and 2022, Amazon admitted in a Senate hearing that it had provided Ring footage to police departments without user consent on multiple occasions. Amazon has since tightened its policies, but the incident revealed how smart home surveillance data can flow outside the home without the resident's knowledge.

Voice Assistants as Always-On Microphones

Amazon Echo, Google Home, and Apple HomePod all use a 'wake word' system: the device listens passively at all times for a trigger word (Alexa, Hey Google, Siri), and only processes and transmits audio after that word is detected. In theory, this means the device only records when you want it to. In practice, it is more complicated. All three companies have acknowledged cases where their devices accidentally triggered without a wake word and recorded private conversations. Amazon and Google both employ human reviewers who listen to a small sample of voice assistant interactions to improve speech recognition — a practice that was disclosed only after journalists discovered it through public records. Both companies now allow users to opt out of human review, but the default was collection first, disclosure second. In 2023, a class-action lawsuit against Amazon alleged that Alexa

devices had recorded children's conversations without consent and stored them for years. Amazon settled for $25 million. The case highlighted the gap between what smart home devices say they do and what they actually do with the data they collect.

Privacy Trade-offs and What You Can Do

The smart home AI landscape involves a genuine trade-off: more convenience and better functionality in exchange for more intimate data collection. A Nest thermostat that doesn't know your schedule is just a programmable thermostat. A Ring doorbell without AI is just a camera. The intelligence comes from the data — and the data comes from you. Users who want to minimize their exposure have real options: physically covering cameras when not needed, using privacy modes (most smart speakers have a microphone mute button), reviewing and deleting stored voice history regularly, and opting out of human review programs. More broadly, understanding what you agreed to in the terms of service before plugging in a smart home device is one of the most practical forms of digital literacy available.

Privacy Trade-Offs in the Connected Home

Every smart home device that uses AI requires a data connection to function. When you ask Alexa to adjust your thermostat or your Ring doorbell detects motion, that data travels to company servers where it is processed and stored. This creates privacy considerations that smart home buyers do not always evaluate carefully before purchase. Amazon, Google, and Apple have all faced scrutiny over how long they retain voice recordings, whether human reviewers listen to clips to improve AI accuracy, and under what circumstances they share data with law enforcement. Ring, for example, built a partnership program with hundreds of police departments that allowed officers to request doorbell camera footage directly. Privacy advocates argue that the aggregate effect of millions of smart home devices creates a surveillance infrastructure that homeowners opted into without fully understanding its implications. Most platforms now offer clearer controls for data deletion, but the defaults still favor data collection.

Energy Management and the Grid-Level Impact

One of the strongest practical cases for smart home AI is energy efficiency at scale. A single smart thermostat saves a modest amount of energy and money. But

when millions of homes use AI-powered thermostats that optimize for off-peak electricity usage, the aggregate effect becomes significant for utility companies managing grid load. Companies like Google Nest have partnered with utilities on demand-response programs, where the thermostat AI automatically pre-cools or pre-heats homes before peak hours, reducing strain on the grid during high-demand periods. Homeowners participating in these programs often receive bill credits. This represents an interesting model where the AI in individual devices is coordinated at a systems level to address infrastructure challenges that no single household could meaningfully impact on its own. Smart home AI, in this framing, is as much a grid management tool as a convenience feature.

The Integration Challenge: Making Devices Work Together

One of the persistent frustrations for smart home owners is interoperability — the ability of devices from different manufacturers to communicate with each other seamlessly. Amazon Alexa, Google Home, and Apple HomeKit have historically used different protocols, meaning a thermostat designed for one ecosystem might not work with a hub from another. The Matter standard, developed collaboratively by major tech companies and ratified in 2022, aims to solve this by creating a common communication protocol that all smart home devices can use regardless of manufacturer. If broadly adopted, Matter would eliminate the ecosystem lock-in that has complicated smart home setups and allow AI assistants from different companies to control the same physical devices. The standard represents an unusual instance of competing technology platforms cooperating to address a shared problem that was frustrating their mutual customers.

Key Information: Smart Home AI Devices

Detail	Information
Nest Thermostat	Launched 2011; Google acquired 2014; learns schedule from behavioral + motion data
Ring Doorbell	Amazon acquired 2018; uses computer vision for person, package, and vehicle detection
Ring Neighbors App	Community footage-sharing platform; documented cases of racial bias in flagging

Detail	Information
Ring + Law Enforcement	Amazon admitted to sharing footage with police without consent multiple times (2020-2022)
Wake Word System	Device listens passively; activates and transmits after trigger word (Alexa, Hey Google, Siri)
Human Review Issue	Amazon and Google both employed humans to review recordings; disclosed only after journalists found it
2023 Lawsuit	Amazon settled $25M lawsuit over Alexa recording children without consent
User Controls	Microphone mute, camera covers, voice history deletion, opt out of human review

Case Study: The Echo in the Kitchen

The Okonkwo family has had an Amazon Echo in their kitchen for two years. The parents, Chidi and Amara, use it for timers, recipes, and playing music. Their 8-year-old daughter, Zara, has started talking to it too — asking questions about homework, telling it jokes, having whole conversations while she does her after-school snack. One evening, Chidi reads an article about the 2023 Amazon children's data lawsuit. He goes to the Alexa app settings and finds, for the first time, a section showing saved voice recordings. There are hundreds of them. Many are Zara's. He reads through Amazon's privacy policy — something he'd never done when setting up the device. He sees a checkbox he'd never unchecked. He calls Amara over. 'We've been sending her conversations to Amazon,' he says. Amara looks at the recordings. 'She told Alexa things she didn't even tell us,' she says quietly.

1. Describe the specific privacy gap that the Okonkwo family encountered. What information were they missing when they set up the Echo, and how did the device's default settings contribute to this situation?

---

2. The reading describes a gap between 'what smart home devices say they do and what they actually do.' How does the Okonkwo scenario illustrate this gap? What responsibility do you think companies like Amazon have in this situation?

Multiple Choice

1. How does the Nest Learning Thermostat build its temperature schedule?

    a) It downloads a schedule from Google's servers based on local weather data

    b) It uses facial recognition to identify which family member is home and adjusts to their preference

    c) It observes behavioral patterns and motion data over time to build a predictive temperature model

    d) Users manually program it during initial setup and it never changes

2. What controversy surrounds Ring's Neighbors app?

    a) It uses significantly more battery power than Ring ever disclosed to its own customers in advertising

    b) It has been used to share footage of people of color doing normal activities, enabling racial bias

    c) It charges users an extra fee to access video after 24 hours

    d) It stores all footage on overseas servers where foreign governments may potentially access it

3. What does the 'wake word' system on smart speakers theoretically mean for privacy?

a) The device only activates and transmits audio after hearing a specific trigger word

b) The device uses facial recognition systems to first identify who is speaking

c) The device will only respond to voice commands issued by registered household members

d) The device records everything said in the home and stores it permanently on servers

Matching

Write the letter of the correct definition on the line next to each term.

Term	Definition
1. ___ Wake Word	A) A community platform built into the Ring ecosystem that allows residents to share surveillance footage with neighbors
2. ___ Computer Vision	B) The pre-configured options a device or service uses unless the user actively changes them — often favoring data collection
3. ___ Ring Neighbors App	C) A practice by Amazon and Google in which employees listen to a sample of voice assistant recordings to improve accuracy
4. ___ Human Review	D) A trigger phrase (such as 'Alexa' or 'Hey Google') that activates a smart speaker's recording and response function
5. ___ Default Settings	E) An AI technique that enables cameras and devices to analyze and interpret visual information in real time

Fill-in-the-Blank

1. Amazon settled a _____ million dollar lawsuit in 2023 over allegations that Alexa recorded children's conversations without consent.

2. Ring cameras use _____ vision AI to distinguish between a person, a moving branch, and a passing vehicle.

3. Google acquired the Nest thermostat company in _____ .

Short Answer

Answer each question in 2-4 complete sentences.

1. The reading says smart home AI involves a 'genuine trade-off.' What exactly is being traded, and who ultimately decides whether that trade-off is worth it?

_____

_____

_____

2. How does the Ring Neighbors app example show that AI technology and human bias can amplify each other's effects? Give a specific example from the reading.

_____

_____

_____

3. Why is it significant that Amazon and Google's human voice review practices were 'disclosed only after journalists discovered them'? What does that reveal about tech company transparency?

_____

_____

_____