

# Smart Lighting System

## Consent to Participate

### Purpose of the Survey

This survey is being conducted to understand participants' knowledge and perceptions of different Internet of Things (IoT) devices and application domains, as well as their awareness of related privacy and security concerns.

### Data Being Collected

We will ask for basic demographic information (such as age range and region) along with your responses to the main survey questions.

### Voluntary Participation

Your participation is completely voluntary. You may choose not to answer any question or exit the survey at any time.

### Anonymity and Confidentiality

Your responses will remain anonymous and confidential. No personally identifiable information will be collected or shared.

### Questions or Concerns

If you have any questions about this survey, please contact

Md Ahnaf - mxa230196@utdallas.edu

Anamika Das - axd240045@utdallas.edu

Tarikul Islam - tarikulcse14@gmail.com

### Consent Statement

By clicking "**Next**" and continuing with this survey, you indicate that you are at least [*minimum age, e.g., 18 years old*], have read the above information, and **agree to participate**.

No direct personally identifiable information (PII) will be collected.

## Section: Demographic Profile

1. What is your age range?

*Mark only one oval.*

Under 18

18 - 24

25 - 34

35 - 44

45 - 54

55 - 64

65 or older

2. Which geographical area do you reside in?

*Mark only one oval.*

North America

South America

Europe

Africa

Asia

Australia/Oceania

Middle East

Other: \_\_\_\_\_

### **Section: Awareness and Understanding**

3. Q1. What is your understanding of the term "**Internet of Things (IoT)**"?

*Mark only one oval.*

Devices connected to the internet that collect and share data

A network of computers communicating via a centralized server

A system of physical devices without internet connectivity

Not sure

4. Q2. What is your understanding of **Cyber-Physical Systems (CPS)**?

*Mark only one oval.*

- Systems where physical processes are controlled or monitored by computer-based algorithms
- Computers that simulate physical processes without any real-world data
- Devices that only communicate between each other locally
- Not sure

5. Q3 . What types of data do you think **IoT** and **CPS** devices typically collect? (Select all that apply)

*Check all that apply.*

- Personal identifiers (name, address, etc.)
- Location data
- Health and fitness data
- Environmental data (temperature, humidity, etc.)
- Behavioral data (habits, patterns)
- Other: \_\_\_\_\_

6. Q4. How do you think data collected by **IoT** and **CPS** devices is used? (Select all that apply)

*Check all that apply.*

- To improve device functionality and performance
- To share with third parties for advertising or marketing purposes
- To enhance user experience by personalizing services
- I don't know

### **Section: Privacy Perceptions**

7. Q5. What privacy concerns, if any, do you have regarding **IoT** and **CPS** devices?  
*(Select all that apply)*

*Check all that apply.*

- Data being shared without consent
- Security risks of unauthorized data access or breaches
- Loss of personal control over collected data
- Unclear data storage practices or retention
- Other: \_\_\_\_\_

8. Q6. Do you think **IoT** and **CPS** devices should inform users about what data is being collected and how it is used?

*Mark only one oval.*

- Yes, always
- Yes, but it should depend on the device or context
- No, it's not necessary for users to be informed
- Not sure

9. Q7. How concerned are you about the security of your personal data when using **IoT** and **CPS** devices?

*Mark only one oval.*

- Very concerned
- Somewhat concerned
- Not concerned at all
- Not sure

10. Q8. What measures do you believe should be taken to protect privacy in **IoT** and **CPS** systems? (Select all that apply)

*Check all that apply.*

- Encryption of data during transmission or storage
- User control over what data is stored or collected
- User authentication for accessing devices or data
- Regular software updates/patches for vulnerabilities
- Strict access controls and auditing of data usage
- I don't know

11. Q9. What does **GDPR** stand for?

*Mark only one oval.*

- General Data Protection Regulation
- Global Digital Privacy Rules
- Government Data Privacy Regulation
- Not sure

12. Q10. What does **HIPAA** protect?

*Mark only one oval.*

- Medical and health-related information
- Home security footage
- Financial account details
- Not sure

13. Q11. Are you aware of any regulations or standards protecting privacy in IoT and CPS systems (e.g., GDPR, HIPAA)?

*Mark only one oval.*

- Yes, I am aware of regulations like GDPR, HIPAA  
 I have heard of them but don't know much about them  
 No, I am not familiar with them  
 Other: \_\_\_\_\_

## Information on GDPR and HIPAA

### What is GDPR?

→ A law in Europe that protects people's personal data and privacy.

### Why is GDPR important?

→ It makes sure companies don't misuse or share your personal information without permission.

### What kind of data does GDPR protect?

→ Your name, email, phone number, address, photos, and even your location.

### Can a company collect your data without asking?

→ No. Under GDPR, they must ask for your clear permission first.

### Can you ask a company to delete your data?

→ Yes. It's called the "right to be forgotten."

### What is HIPAA?

→ A U.S. law that protects your health information and privacy.

### What kind of information does HIPAA protect?

→ Your medical records, test results, doctor visits, and health insurance details.

### Can your doctor share your health information with anyone?

→ No. They must keep it private unless you say it's okay.

### Why is HIPAA important?

→ It keeps your personal health details safe from being misused or leaked.

### Can you see your own medical records?

→ Yes. HIPAA gives you the right to view and get copies of them. GDPR (General Data Protection Regulation)

14. Q12 . Would you be willing to share personal data with **IoT** and **CPS** devices if there was a clear benefit to you (e.g., better services, personalization)?

*Mark only one oval.*

- Yes, if the benefits are significant
- Yes, but I need to know how my data will be protected
- No, I prefer not to share my personal data
- Not sure

15. Q13. What would make you trust **IoT** and **CPS** devices more regarding privacy?

*Mark only one oval.*

- Transparency about data collection and usage
- Control over data sharing and access settings
- Clear privacy policies with user-friendly knowledge
- Third-party certifications or audits on security practices
- Other: \_\_\_\_\_

16. Q14. Do you think **IoT** and **CPS** technologies have a significant impact on privacy in society today?

*Mark only one oval.*

- Yes, I believe they have a significant impact
- No, I don't think they affect privacy much
- I'm not sure

17. Q15. Would you like to see more information about privacy and data usage in **IoT** and **CPS** systems?

*Mark only one oval.*

- Yes, I would appreciate more resources
- No, I feel well informed
- Not sure

### **Section: Device/System Specific Questions**

18. Companies may use the collected data for different purposes – some to improve your experience, and others for business or marketing. Based on what you know, how do you think this collected data is typically used? (e.g., service improvement, targeted ads, sharing with utilities, selling to third parties, etc.)

---

---

---

---

---

19. Q16. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Bulbs**? (Select all that apply)

*Check all that apply.*

- Brightness levels: Records of light intensity settings over time.
- Ambient light conditions: Environmental light readings detected by sensors.
- Motion detection logs: Movement data recorded by motion sensors in the bulb.
- Temperature readings: Ambient temperature measured near the bulb.
- Power consumption data: Energy usage data for each bulb.

20. Q17. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Light Switches**? (Select all that apply)

*Check all that apply.*

- Touch interactions: Logs of manual on/off or dimming actions.
- Occupancy detection data: Room presence data recorded via occupancy sensors.
- Switch usage patterns: How often and when switches are activated.
- Proximity-based control triggers: When lights activate/deactivate due to nearby movement.
- Temperature readings: Ambient temperature recorded near the switch.

21. Q18. How comfortable are you with sharing your data with IoT manufacturers or third parties regarding **Smart Lighting Systems**?

*Mark only one oval.*

- Extremely uncomfortable
- Somewhat uncomfortable
- Neither comfortable nor uncomfortable
- Somewhat comfortable
- Extremely comfortable

## Section: Privacy Implications

### **Implications: How Smart Lighting Systems Use Your Data**

Smart bulbs and switches don't just turn lights on or off—they monitor environmental conditions, your habits, and even movement in your home. This information can help optimize energy usage, automate lighting, and improve comfort—but it can also be shared or monetized in ways you might not expect.

- ◆  **Targeted Recommendations:** Dim lights often? Expect ads for mood lighting or décor. High nighttime usage? See promotions for blackout curtains or energy-saving bulbs.
- ◆  **Data Sharing:** Brightness levels, motion detection, and usage logs may be shared with manufacturers, advertisers, or smart home platforms.
- ◆  **Paid Features:** Advanced scheduling, adaptive lighting based on circadian rhythm, or detailed energy reports may require a subscription.
- ◆  **Behavioral Profiling:** Motion and occupancy sensors can reveal your daily routines, when you're home, and when certain rooms are used most.
- ◆  **Environmental Tracking:** Ambient light and temperature readings can be valuable for energy efficiency data or even urban planning research.
- ◆  **Third-Party Access:** Data may be shared with insurers, property managers, or law enforcement—sometimes without clear consent.

### **What This Means for You:**

Smart lighting can be a powerful energy saver and comfort enhancer—but it also tracks patterns in how and when you use your home. Regularly review privacy settings and understand how brightness levels, motion data, and usage patterns are collected and shared.

## Section: Device/System Specific Questions after Understanding Implications

"After reading **Implications: How Smart Lighting Systems Use Your Data** you will be asked the same set of **Device/System Specific Questions** again. Any changes you make will reflect how your views **shifted after learning** about these implications."

22. Q19. Which types of data are you comfortable sharing with IoT manufacturers or third parties regarding **Smart Bulbs**? (Select all that apply)

*Check all that apply.*

- Power consumption data: Energy usage data for each bulb.
- Temperature readings: Ambient temperature measured near the bulb.
- Motion detection logs: Movement data recorded by motion sensors in the bulb.
- Ambient light conditions: Environmental light readings detected by sensors.
- Brightness levels: Records of light intensity settings over time.

23. Q20. Which types of data are you **comfortable** sharing with IoT manufacturers or third parties regarding **Smart Light Switches**? (Select all that apply)

*Check all that apply.*

- Temperature readings: Ambient temperature recorded near the switch.
- Proximity-based control triggers: When lights activate/deactivate due to nearby movement.
- Switch usage patterns: How often and when switches are activated.
- Occupancy detection data: Room presence data recorded via occupancy sensors.
- Touch interactions: Logs of manual on/off or dimming actions.

24. Q21. How comfortable are you with sharing your data with IoT manufacturers or third parties regarding **Smart Lighting Systems**?

*Mark only one oval.*

- Extremely uncomfortable
- Somewhat uncomfortable
- Neither comfortable nor uncomfortable
- Somewhat comfortable
- Extremely comfortable

25. Challenges? What you will be missing due to limiting these data accesses?

---

---

---

---

---

---

---

---

---

---

---

---

This content is neither created nor endorsed by Google.

Google Forms