**Exploring How Privacy and Security Factor into IoT Device Purchase Behavior**

**ABSTRACT**

Despite growing concerns about security and privacy of Internet of Things (IoT) devices, consumers generally do not have access to security and privacy information when purchasing these devices. We interviewed 24 participants about IoT devices they purchased. While most had not considered privacy and security prior to purchase, they reported becoming concerned later due to media reports, opinions shared by friends, or observing unexpected device behavior. Those who sought privacy and security information before purchase reported that it was difficult or impossible to find. We asked interviewees to rank factors they would consider when purchasing IoT devices; after features and price, privacy and security were ranked among the most important. Finally, we showed interviewees our prototype privacy and security label. Almost all found it to be accessible and useful, encouraging them to incorporate privacy and security in their IoT purchase decisions.

**EXISTING SYSTEM**

Labels are used in numerous applications such as the nutrition facts label for foods, fuel economy and environment label for cars, European Union (EU) energy label for office appliances, Power Content Label (PCL) for electricity, Energy Guide label for home appliances, and Lighting Facts label for light bulbs. Researchers have found that standardized labels are a promising approach for informing consumers about privacy: privacy “nutrition labels” on websites, privacy meters in search engines, and a “privacy facts” checklist in an app store have been shown to impact study participant decision making. However, labels proposed in this prior work were not designed for IoT devices. In addition, those labels focused solely on privacy and did not consider security factors.

**Disadvantages of Existing System:**

1. Labels proposed in this prior work were not designed for IoT devices.
2. Labels did not consider security factors.

**PROPOSED SYSTEM**

We conducted in-depth semi-structured interviews with 24 participants who had purchased at least one IoT device (smart home device or wearable). We explored interviewees’ understanding of privacy and security issues associated with IoT devices and factors they considered when purchasing their device. At the end of each interview, we displayed prototype IoT security and privacy labels that we developed, and discussed them with interviewees. Finally, we conducted a 200-participant Mechanical Turk (MTurk) survey to probe the influence of privacy and security information when making IoT purchase decisions.

**Advantages of Proposed System:**

1. From our findings, we distill recommendations for the design of privacy and security labels that enable consumers to make informed IoT device purchase decisions.
2. Our findings on consumers’ interest in IoT nutrition labels, and ways to make them more useful, are important and timely contributions as policy makers debate new IoT privacy and security regulations

**SYSTEM IMPLEMENTATION**

**System Architecture**



**Figure 1: Prototype label for a hypothetical security camera with poor privacy and security practices**

**SYSTEM REQUIREMENTS**

# Hardware Requirements:

# Processor - Pentium –IV

* Speed - 1.1 GHz
* Ram - 256 MB
* Hard Disk - 20 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java