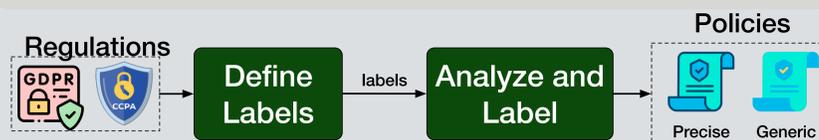


Motivation

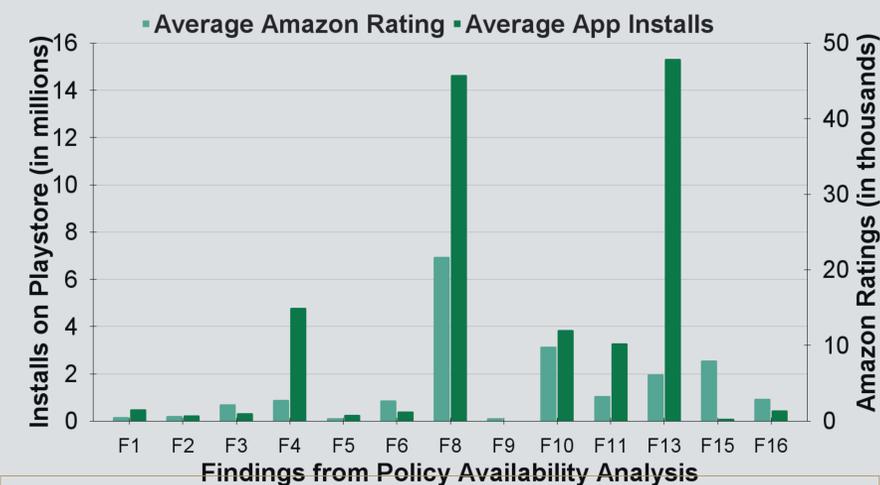
- Smart home device usage data can be used to profile users.
- Users have **significant privacy concerns** about IoT devices, hindering market adoption.
- Privacy policies** are the primary medium for conveying data handling practices of a company.
- Understanding the privacy policies of IoT devices helps us **gauge the privacy guarantees promised to users**.
- We perform the **first large-scale evaluation of vendor-provided smart home privacy policies**.

Content Analysis



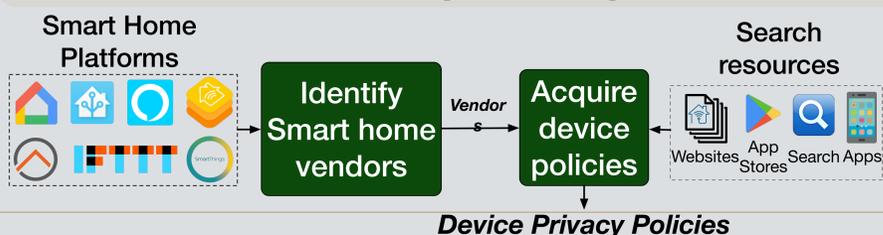
- 74/292 privacy policies **do not disclose specific device or device data** when discussing data collection, e.g. “service usage information” or “sensor information”. \mathcal{F}_6
- 186/292 privacy policies **do not discuss sharing practices** of data collected from smart home devices while 70/292 do not specify with whom data is being shared. \mathcal{F}_{10} \mathcal{F}_{11}
- Existing state-of-the-art **privacy policy analysis tools fail to properly reason** about 196/292 smart home device policies due to structural and semantic challenges. \mathcal{F}_8
- 8/292 vendors explicitly state they do not collect any information. 6 do not discuss sharing at all. \mathcal{F}_9

Impact Evaluation



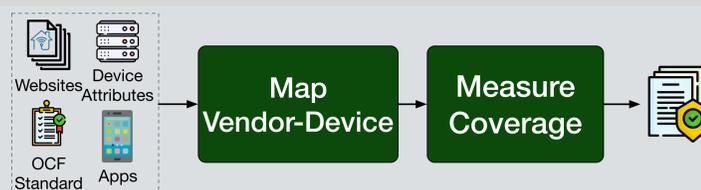
- Our findings impact vendors whose products are **used by millions of users** as indicated by our impact metrics.

Availability Analysis



- 63/596 vendors **do not provide any privacy policy** while 225/596 do not provide policy that apply to smart home products. We were able to obtain privacy policies for 292 vendors. \mathcal{F}_1 \mathcal{F}_2
- 160/596 vendors **did not post privacy policy links on their homepage** marked with “privacy” or similar phrases, which may violate privacy regulations. \mathcal{F}_5
- Even in cases where smart home policies were available, they can be very **difficult to obtain**, with 42/292 requiring us to execute vendor’s apps to obtain policy while 21/292 policy were available only in Google Play Store. \mathcal{F}_3 \mathcal{F}_4

Coverage Analysis



- 50/292 vendors discuss device data **only for a subset of the devices** they sell in their privacy policies. \mathcal{F}_{13}
- Vendors **do not differentiate their privacy disclosures** for devices that produce similar data but have vastly different privacy implications e.g., disclosure concerning video doorbell and baby monitors. \mathcal{F}_{14}
- Vendors 29/292 vendors describe the collection of device data **precisely**, but also discuss irrelevant data possibly due to the use of templates. \mathcal{F}_{15}
- Broad statements** used to describe device data collection may not always denote insufficient precision. \mathcal{F}_{16}

Takeaway

- Our findings motivate the **need to improve precision and completeness** at which device data is discussed in smart home privacy policies.
- Our accessibility analysis **highlights the user burden in effectively evaluating the privacy repercussions** of smart home devices.
- Our study motivates the need for the **effective standardization of privacy policies**, so that automated tools can be developed to reduce cost and effort for both vendors and consumers.

Responsible Disclosure

We have reported our findings to **506 vendors**. We received **113 responses**, out of which 71 were automated responses, 6 reported that they are in the process of updating privacy policies and 9 vendors had already updated their privacy policy.