Personal Privacy and Data Security: How Secure is Information Observed and Recorded by Amazon's Alexa?

Names: Laura Schuck

Background of the Problem and Motivations:

As the Internet of Things (IoT) expands into every aspect our day-to-day lives, more and more of our personal information is being stored and/or processed by third parties. Millions of people have brought devices containing voice-controlled assistants into their homes. With devices containing Amazon's Alexa, users can control televisions, lights, security systems, and so much more.

The convenience afforded by voice-controlled assistants requires users to give up a level of privacy. Personal conversations, bank account and credit card information, and medical information are among the data many people share with assistants such as Google Home, Apple's Siri, and Amazon's Alexa. The laws governing these companies' use of personal recordings are generally lax or nonexistent in the US, though the European Union has enacted laws such as the General Data Protection Regulation.

Many people may not realize their interactions with assistants such as Amazon's Alexa are recorded. Each time a user engages Alexa with the wake word ("Alexa" by default), the light on the physical devices turns blue, indicating a recording is occurring. While users may be aware of the instances in which they intentionally engage Alexa, it is common for Alexa to misinterpret words in a conversation as the wake word. This commences a recording the owners may remain unaware of. All recordings are then sent to the cloud for processing. Amazon has employees that manually listen to and transcribe recordings in order to improve Alexa.

As recently as August 2020, vulnerabilities have been found with Amazon's Alexa. There have been instances in which Amazon has suffered data breaches with users' Alexa information. Beyond the recordings themselves, other data can be stored including IP addresses and location information. Data breaches with that information could put users at risk of attack. Because Amazon's Alexa sends all audio recordings to the cloud for processing rather than processing in the physical device, users are at an increased level of risk.

Objectives:

In my work, I aim to explore the security of data collected and processed by Amazon's Alexa. A review of the current laws and governance around data protection with voice-controlled assistants will be conducted. I will also analyze the default privacy and data collection settings as well as the options provided for users to customize privacy settings for Alexa devices. How data is transmitted and stored, as well as data and security breaches of Alexa recordings and information is another area that will be explored. Additionally, I will review the security measures and review processes required for an application or skill to be introduced to the market.