**AMAZON ALEXA SCANDAL- A Reality Check on the VPA Market**

-by Nikita Jangid (MSc 1st Year)

Many of us have heard the phrase Hey Siri or Okay Google, be it advertisements or our mobile phones, seldom paying attention to these features which help us with simple tasks within our mobile devices. These are called Virtual Personal Assistants (VPAs) or simply virtual assistants. As the name suggests, these are personal assistants within our mobile phones which help us with simple tasks such as setting an alarm, calculating numbers or doing a quick search. Not only phones, these assistants are also deployed in smart home devices and smart speakers. The smart home devices are used to monitor and control lighting, heating and security systems thereby creating a home automation system. Some commonly known virtual assistants include Siri by Apple, Google Assistant by Google, Alexa by Amazon, Cortana by Microsoft, and Blackberry Assistant by Blackberry and Bixby by Samsung. Virtual personal assistants deployed in smart speakers and home devices are continuously switched on since they monitor conversations for voice commands. With such home devices monitoring different home activities, they have enormous power to access ones daily household conversations which may include private and sensitive information. This may lead to privacy breach and information leakage. One such incident took place in the house of a family residing in the United States and is now famously called the Alexa Scandal.

**Amazon Alexa Scandal**

A couple in Portland, Oregon, received a nightmarish phone call, about their Echo devices being hacked. Apparently, ]one of the Amazon.com Inc.”Alexa-powered Echo devices in their home had silently sent recordings to the caller, without the couple’s permission. The caller, who happened to be an employee of the husband, was in the couple’s contact list. The couple used Amazon’s voice-activated devices throughout their home to control heat, lights and the security system.

**Amazon’s Explanation**

An Amazon spokesperson told the news station, ”Amazon takes privacy very seriously. We investigated what happened and determined this was an extremely rare occurrence. We are taking steps to avoid this from happening in the future. and gave the following explanation: Echo woke up due to a word in background conversation sounding like Alexa. Then, the subsequent conversation was heard as a send message request. At which point, Alexa said out loud To whom? At which point, the background conversation was interpreted as a name in the customers contact list. Alexa then asked out loud, [contact name], right? Alexa then interpreted background conversation as right. As unlikely as this string of events is, we are evaluating options to make this case even less likely .”

VPA is a computer program that uses Artificial intelligence technology which helps to start a conversation with humans through auditory or textual methods. To achieve human-like interaction AI includes many methods and technologies like machine learning, neural network, natural language processing, cognitive computing, speech recognition, handwriting recognition etc.

VPA’s can be very helpful to us but there are some problems related to VPAs that make us think whether these intelligent systems are reliable or not.

Whenever one uses the services of a virtual assistant, they will be passing along confidential information and records which potentially exposes your personal details, such as contact list, names or location and we are unaware of whether this data is stored or deleted. Many cases of information being leaked from online databases have been witnessed and can be easily done by humans in the past which poses serious security threats. Virtual helpers like Siri and Cortana are useful, but does not keep our questions private. As these assistants are always connected to the internet, the risk multiplies if they have access to passwords and sensitive information within apps linked to them in a manner that they are vulnerable to phishing. There is no surety that the task given to the device will be completed or not because the state of the request cannot be monitored due to absence of a screen or other physical record-keeping system.

The virtual assistants may be the new trend and be helpful, but data security, privacy breach, lack of reliability, limited responses and high price highlight the negative aspects of such assistants, which cannot be ignored. They cannot replace tasks done manually or by humans and are unreliable in their functioning and responses. Privacy and data security are sensitive areas about which most people are unaware, and are uninformed about the probable security threats and apparent data phishing which might take place by continuously using such devices. All these negative aspects have led to the reality of these assistants in the real world.

References

<https://www.vox.com/2018/5/24/17391480/amazon-alexa-woman-secret-recording-echo-explanation> ( Amazon’s explanation)