Amazon Echo Security Review

The Amazon Echo is a smart speaker made by Amazon that was introduced to add convivence for multiple everyday tasks. These tasks involve many trivial aspects of life such as setting a timer, turning up the volume of your music, or checking the time. The difference between doing these tasks with an Amazon Echo is that they all become hands free tasks with Amazon Alexa's voice commands. On top of the many commands offered while the device is offline, the Amazon Echo also allows for WIFI connectivity. Connecting an Amazon Echo to the internet allows for many more features such as checking the weather, ordering a product off Amazon.ca, or connecting it to other smart home devices like lights or thermostat. On top of all the stock features that Amazon offers, Amazon allows third-party developers to use an API for interfacing with Amazon Alexa to create apps that have voice command features. These voice command features work by saying Alexa followed by the command you want to use, which shows that the microphone on the Amazon Echo is always listening and waiting for a command. The always-on microphone as well as allowing third-party developers to create apps for Amazon Echo, assuming Amazon does not check the source code of these apps for nefarious actors, opens possible security and privacy concerns surrounding the product.

Two of the main principles that makes a house feel like a home is security and privacy. All sorts of personal information is disclosed when you are in your home, and there are many aspects of peoples lives they want to keep private. Without this feeling of privacy, people do not feel comfortable in their own house. Another aspect of security in a home is its wireless network. Having internet has become a necessity in the past decade with the most common implementation being WIFI. Making sure no nefarious software has access to a homes wireless network is incredibly important in preserving a person's personal data and privacy. An Amazon Echo runs into conflict when discussing security and privacy in a person's home. Having a microphone that must be always listening is in direct conflict with the sense of privacy someone has in their home when discussing sensitive personal subjects. On top of always listening, Amazon Echo connects to a home's wireless network while allowing third party developers to create apps for it. This leads to the possibility of a nefarious app developer gaining access to your wireless network, which could lead to personal data being accessed. This could be accomplished by creating an app that seems harmless on the surface when in reality the app is constantly recording all audio from the Amazon Echo's microphone.

These possible security threats can easily be resolved. In the case of a home's wireless network, in order to defend from these possible nefarious actors, you could have the Amazon Echo check for unusual network traffic going to and from it. If something outside the normal network traffic is noticed, the app that sent or received it can be disabled. Another way of stopping nefarious app developers would be to do a thorough review of the source code before allowing it to be downloaded from Amazon. The likelihood of there being a nefarious app developer that could get away with this without anyone's knowledge of it is low. If people stick to reputable apps that have already had security reviews, their wireless network should be safe. However, having a microphone that is always recording should be of

concern. What is discussed in the assumed privacy of a home could still be recorded and stored by Amazon itself.

The Amazon Echo provides many conveniences in everyday life. From setting a timer with your voice while your hands are dirty from cooking to setting tomorrows alarm while laying in bed, these conveniences have been happily adopted by many people. With these aids comes a possible breach in privacy that should not go unnoticed. What an Amazon Echo records and what they do with that data can not be fully known. Most people assume that it is just sold to advertising agencies to help market products to you that you are more likely to buy. But what if that data got into the wrong hands, such as a foreign government? It has been shown that the Chinese government spies on its citizens oversees. What if Amazon sold Echo recordings of Chinese citizens to the Chinese government for their use to control dissent abroad? People need to be aware of the information they may be unknowingly providing and the possible privacy risks in this new age of the internet, and that starts with acknowledging the possible security and privacy risks associated with new products like the Amazon Echo.