COVA CCI Undergrad Cyber Research

Nana Jeffrey

Norfolk state University

April 14, 2022

Is your digital assistant your worst enemy? Modern technology has impacted our lives in a positive way making tasks that were once time consuming become more convenient. For example a few years ago writing down your grocery list with a paper and pen was a norm, now with technology we have access to IoT devices such as smart fridges that can inform us on what items are low in stock, send a message to our digital assistants such as iOS Siri and Amazon's Alexa to remind us to buy those groceries. Although these digital assistants have helped make our daily lives more convenient, they have access to a lot of users' information. As digital assistants continue to advance and become a part of our daily lives, our data will continue to be susceptible to attackers stealing information. It is important for companies to implement privacy tools and guidelines in order to keep our users safe from these types of attacks.

Digital assistants are voice activated software programs that perform a variety of tasks for users. Some examples of digital assistants are Google assistant, iOS Siri, and Amazon's Alexa. Digital assistants work together with IoT devices, which are devices with embedded technology that can connect to a network such as a google home to perform many tasks. These tasks can include playing music, checking the weather at any desired location, adding items to a shopping list, sending reminders for upcoming appointments and much more. As stated previously digital assistants can perform many tasks that may not seem grand but have a positive impact on our daily lives. For example, a user who has been diagnosed with early stages of dementia can use her mobile devices to say “Hey Siri, set a reminder to pick up my medication” and Siri would reply with “Ok, setting reminder to pick up medication,” Siri might also ask the user for extra details on what day they should set the reminder, and if they want an alarm to be set 30 minutes prior to their task. If the user had written this task down on paper she could have lost it. Allowing her digital assistant to set the reminder on her phone limited the risks of her forgetting to pick up

her prescription had she chosen a different option. Other than our daily lives, the workforce is another area digital assistants have made their presence known. For instance e-commerce businesses may use digital assistants in the form of chat boxes to provide 24/7 customer service care. In the healthcare field we have seen an increase of personal digital assistants (PDA). PDA's are small pocket sized computers that have been used as personal organizers. These have allowed medical professionals to have access to evidence based knowledge within seconds in order to provide the best care for their patients. Despite the many positive impacts digital assistants have had on our daily lives, and businesses, there are some negative impacts as well. Imagine living in a smart home where numerous IoT devices are connected to your homes' network. If an attacker were to use Alexa to hack into your Amazon Echo speaker, they could have access to all the other devices it's connected to in your home, this could be your security system, appliances, and even thermostat. In the workforce an attacker could hack into a digital assistant located on an e-commerce website to access credit card information that you saved to your laptop.

With the many tasks digital assistants are able to perform, the posing question is how much of a user's data is taken into account in order to perform these tasks. Let's take a look at Amazon's Alexa. Think about everything you've ever asked Alexa, or even the times where Alexa responded to something you never even said. All that data is being recorded and kept as a copy for Amazon. Amazon has had numerous battles with lots of consumers posing the question about why and who is listening to users when they use their echo device. "The Amazon Echo, despite being small, is a computer - its a computer with microphones, speakers, and its connected to the network." (Hamza Shaban 2018) so long as it's connected to the network your data is being recorded. Alexa is a voice assistant that is connected to a lot of IoT devices. These devices are connected to a numerous amount of things in a person's home such as security cameras, and

light systems. For instance, a Philips Hue light keeps track of everytime you switch on or off your light. A chamberlain MyQ garage opener keeps record of every time your door opens and closes, the Sonos speaker picks up on your listening habits by keeping track of the music you listen to, how often you press pause on a song and even when you increase the volume on your device. Most of this data collected by these IoT devices are kept indefinitely by these companies and shared with Amazon. Although Amazon claims that they only keep records from Alexa to improve the products and not sell them, they aren't stopping companies from sharing users data with them. According to Beatrice Geoffrin, director of Alexa Privacy, “Alexa is always getting smarter, which is only possible by training her with voice recordings to better understand requests, provide more accurate responses and personalize the customers experience,” (Fowler, 2018) Users data are drastically becoming the price of entry for devices that want to join with Alexa. Although Apple placed more privacy aspects for the users benefits, Siri is still collecting data from recordings on a smaller scale. Compatible devices that are connected with Alexa share any and everything going on in a user's home, whereas software by Apple such as homekit doesn’t.(Fowler,2018) However, that does not mean users are safe from their data being used, in fact they still keep copies of conversations with Siri. According to Apple's legal page, When you use Siri, Apple stores transcripts of your interactions with Siri and may review a subset of these transcripts to develop and improve Siri and dictation, and other language processing features like voice control.

Despite the fact that the data being collected by Siri and Alexa are being used to improve these devices, the reality is, the amount of users data that digital assistants have access to may be causing users to be susceptible to attacks. As previously mentioned, there are many IoT devices that are compatible with Alexa. Phrases such as “Alexa turn on the lights,” or “Alexa open

garage door," allow Alexa to work with these devices in order to fulfill the user's commands. These phrases are all being recorded and accessed by Amazon employees. Amazon employees not only have access to these transcripts of recordings taken by Alexa but they also have access to the specific location these devices are made in. (Fowler, 2018) For example, You may say "Hey Alexa what's the weather?" and Alexa might respond back with "Clear skies with a high of 80 degrees." This interaction with Alexa has not only recorded what you sound like, but also the location of where you live. Digital assistants have a lot of access to users' information that can be stolen. Imagine if an adversary were to get ahold of those transcripts that Amazon keeps. Even though user data is used to help develop digital assistants such as Siri and Alexa, it could also lead to users' information being stolen by adversaries. For example, If an ex-employee at Amazon that worked on the Alexa project decides to take action against the company by stealing users information and sell it for their own malicious or financial intent, that employee can access these recorded transcripts, gain information on where you live, the type of questions you ask Alexa and know the day to day habits in your home. Some of this data may include knowing what times your garage closes and opens, how often lights are turned on and off in your home, the temperature you like your home to be in, your listening habits and much more. All of this information about the user could be stolen, used to create a marketing profile and sold to third parties for their own financial gains. Another example of how adversaries can access users' data is through Siri shortcuts. Due to the IOS 12 update, Apple introduced shortcuts for apps with the help of Siri which can complete a wide variety of tasks. However, according to IBM senior researcher John Kuhn, by using shortcuts a hacker can easily use Siri's voice for ransom campaigns that would scare users into believing that their personal data has been stolen from the phone. Malicious Siri shortcuts scripts can also be sent automatically to the entire contact list of

the victim via messages, appearing as a link. (Daniyal Malik, 2019) Data is important, it's how companies create tools that can make our day to day lives easier, however it runs the risk of adversaries hacking into these devices and stealing user information for their own malicious intent. According to Lou Basenses, Descriptive Tech Research founder and chief analyst, “We are giving them unfettered access to our data and look, they can't resist the temptation. Data is a drug to big tech. It allows Google and Facebook to serve you better ads and to think that they are not going to use this data and that it’s just going into the cloud being crunched by algorithms and not be put into their business I think is a little bit naive,” (Tuttie Devukaj, 2019) It is inevitable that companies are going to collect data from users, after all, data is needed in order to create tools to help improve our lives.

As discussed there are many ways an adversary can hack into digital assistants to obtain users data. With data comes the need for protection and privacy. How can companies implement privacy tools and frameworks to better protect users from digital attacks? Let's look at some of the frameworks Apple and Amazon have in place for their users. In August of 2019, Apple put out a statement about improving Siri’s privacy protection. The article mentioned how when Apple stores Siri data on their servers, they don't use it to build a marketing profile or sell it to anyone. As stated previously, they make sure that Siri data is only used to improve Siri. For example if you ask Siri to read your message out loud Siri simply instructs your device to read aloud your unread message. The contents of your message aren’t transmitted to Siri servers. (Apple, 2019) By doing this Apple is ensuring that the data being collected is not being transferred to third parties. Another way Apple implements privacy tools and frameworks on Siri is by using random identifiers. Random identifiers is a long string of letters associated with a single device to keep track of data while it's being processed rather than tying it to your identity

through your Apple ID or phone number. After 6 months the device's data is disassociated from the random identifier. When it comes to Alexas privacy protection Amazon has a slightly different approach. Amazon emphasizes to users that they have the option to turn off these devices that are collecting their data and give you the option to personalize your Alexa privacy settings and even provide tips. Some of these tips include:

1. View, hear, and delete your recordings
2. Review and manage your smart home device state history
3. See and update the Alexa skills that you've granted permission to access specific data
4. Manage how you help improve Alexa.

Here, Amazon is complying with the General Data Protection Regulations (GDPR) law that requires companies to ask for some permission to share data and gives individuals rights to access, delete, or control the use of data. Amazon and Apple have adapted an optional style of privacy and protection when it comes to user data. Their method relies on giving users the option to not be recorded through digital assistants. However, giving users the option to simply turn off their digital assistants shouldn’t be the only form of protection users have against digital assistant attacks. Given that adversaries can use Siri to hack into user’s phones, companies need to implement better privacy tools and frameworks that can protect users from these types of attacks. Most of the technology laws are catered to situations that happen if an adversary was to breach a company's database, or giving users the right to have access to their data that companies are using but there aren't a lot of laws that handle users data being stolen by an adversary through a product that they've bought. If a user trusts that their data is protected through a specific device that they've purchased from a reliable company and their device gets hacked a user should be

able to take necessary action and receive some sort of benefit from the company or on a state level. According to the International Comparative Legal Guides, the federal Computer Fraud and Abuse Act (CFFA), 18 U.S.C 1030 is the primary mechanism for prosecuting cybercrime, including hacking. This act provides for both criminal and civil penalties; these charges can be anywhere from 10-20 years. (McNichalson, 2020) Other acts such as The Consumer Privacy Protections Act of 2017 was designed to ensure the privacy and security of sensitive personal information to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information and to enhance law enforcements (IT Governance inc. 2022) We see examples of that through Apple and Amazon's privacy implementations with Siri and Alexa. However, giving users the option to just turn off their sharing digital assistants isn't enough. From the governance side, more laws need to be implemented in order to protect users from digital assistant attacks. These laws should include insurance on a user's data if their data has been stolen through digital devices. From a company standpoint, they should focus on preventing leaks, keepings their information confidential not only with employees but manufacturers of their products as well. Companies could also adapt Apple's random identifier tactic when creating their digital assistants. Lastly, from a user standpoint, disable digital assistants and limit access to your device. It might be annoying to do things Siri could do instantly by ensuring that a minimum amount of your data is being accessed and shared could lead to your devices being less supsectibel to digital assistant attacks.

Digital assistants have improved the day to day lives of consumers, completing a variety of tasks such as setting reminders to turning the lights off in a room. Even though digital assistants have proven to be very useful, they also are susceptible to being hacked. The more technology advances the more our data is needed to create and improve technology. But the

amount of data being accessed by companies through digital assistants can be alarming, especially when they're capable of recording personal conversations. Moving forward, not only do users need to have access to options regarding their personal data but more laws need to be implemented for specific types of cyber attacks on state and national level.

Work cited

https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/

https://www.foxbusiness.com/technology/apples-siri-is-eavesdropping-on-your-conversations-putting-users-at-risk

https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/

https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/

https://rn-journal.com/journal-of-nursing/how-personal-digital-assistants-can-increase-the-quality-of-nursing-care-provided-in-the-hospital-setting

https://marketbusinessnews.com/financial-glossary/digital-assistant-definition/

https://observer.com/2017/06/siri-voice-assistants-data-collection-speech-recognition/

https://www.digitalinformationworld.com/2019/02/apple-siri-voice-shortcuts-can-be-hacked.html

https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa