Information Technology in a Global Society Extended Essay

To what extent can we judge the value of virtual assistants supporting our lives, compared with the known impacts on user's privacy and anonymity through corporate surveillance?

Word count : 3929 words

Table of Contents

Introduction

Back in 2011, I lived in India, but the time difference didn't stop me from watching the unforgettable keynote when Siri was introduced also called the "intelligent assistant". Today, not only digital immigrants but digital natives rely on virtual assistants for their day-to-day tasks. I came across these terms in my ITGS class, digital natives refers to the people who are born into the digital world and digital immigrants are the people who were fascinated and adopted the various aspects of technology (Prensky). However, there is a fine line between these two terms. There is a continuum rather than a rigid dichotomy between digital natives and digital immigrants, and this continuum is best conceptualized as digital fluency. (Wang et al. 1]) Breaking the market down by generations, 41.1 percent of U.S. Millennials use smart speakers, followed by 34. percent of Gen X, and 17.6 percent of Baby Boomers (Kesten).

I have always been fascinated by what Apple offers to the world, but a concept of human interaction with the complexities of tones, languages, multiple meanings, and even accents amazed me. This innovation made me read more about the subset of Artificial intelligence and Machine learning which went behind it. One of the other reasons, Siri caught the

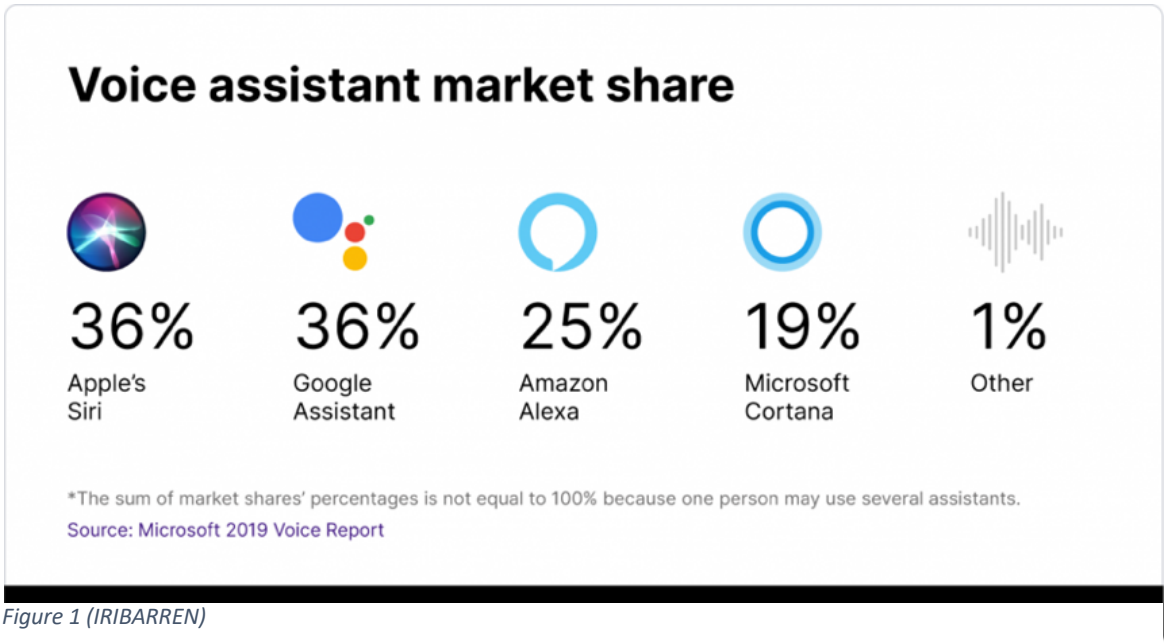


Figure 1 (IRIBARREN)

commoners' attention was because it was an inbuilt e-driven interface at your service. It was the first one but also the most accessible one even today.

Not long after, Siri began to share its markets with Microsoft's Cortana and Amazon Alexa. We were overwhelmed with this innovation, but not for long. I encountered an article with the title "I'm not sure I understand you" (Tripp Mickle). It caught my attention for one reason, which was I could relate to that phrase, and I knew it wasn't just the Indian accent but also many other communities globally which I will discuss about further in my essay. This is a problem because it sets limitations to what the user can use the device for then, creating a divide of experiences in various stakeholders. This is when the population recognized the negative implications and certain inabilities of virtual assistants. Starting from poor voice recognition to issues regarding privacy flooded over the news. This technological innovation's initial aim was for a better and leisure life, however, it now is considered under "surveillance capitalism", which is defined as a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales (Zuboff). After coming across articles regarding the same issue for other virtual assistants such as "Amazon Alexa", "Google home pod" and reading court case laws in which these assistants played a role as substantial evidence(Sui). The key idea we take from this case is that, it was the turning point which made a number of users realize that Alexa, the voice service enabled echo device stores recordings and transcripts from their interactions. However, the interesting counterargument here is that, "surprisingly plausible" that Alexa is protected by the First Amendment (Brewster). He said this because Amazon Alexa strictly denied to share the recording and continued to abide by their privacy policies. Eventually, the user gave amazon the permission and the company dropped the case.

After coming across such implications of this device, I asked myself a simple question, why do people choose comfort over privacy? Hence, in-depth with reference to the ITGS triangle, I framed my question as "**To what extent can we judge the value of virtual assistants supporting our lives, compared with the known impacts on user's privacy and anonymity through corporate surveillance?".** My aim is to thoroughly analyze, the technology behind virtual assistants and how corporates evaluate their policies to compensate the extensive user interface and users' outlook regarding plausible social and ethical concerns.

Overall, this topic is also interesting because virtual assistants hold high potential to be the most used user interfaces in future machines and technological developments, some believe that it will power the future workforce (Brickner).

Methodology of Research

Primary Research

I chose two different aspects to explore to get different perspectives. The first one was a survey based on the usage of virtual assistants; this survey was filled by forty seven users of various virtual assistants. This survey was anonymous however, the only personal information asked was the respondent's age. Many different outcomes are expected, the older age brackets might be more conscious about their data, at the same time more informed about the risks. However, digital natives might only see the leisure aspect of the assistants as they are lured by the evolving technology and like the idea of being reliant on it in their daily life. I will compare my results with the data I obtained from a secondary research source, who conducted a similar survey, however more detailed and with a larger number of sampling data, as my survey's sampling data is relatively small and concentrated in a similar geographical locations, which are Singapore and India, covering only the Asian continent. This restricts certain opinions and perspectives because Asian countries usually receive latest technology a bit later and certain skills and apps are not always compatible.

The second method was an Interview with an Expert of the Computer Science field, who uses virtual assistants greatly in his daily life. This interview will help support and justify my survey's result as the interviewee has a comprehensive understanding of the technology behind virtual assistants , so I decided to keep the questions pretty similar to the survey.

Secondary Research

I started out with carefully reading back few of the articles I came across before. Most of them discuss about the privacy concerns but don't touch upon the reasons why users continue to use it. I started out with reading about the virtual assistants on their actual developer website to understand the technical side of it. Then made use of University databases, Jstor, Google Scholar, etc. I narrowed down my research with the use of advanced search, using keywords such as "virtual" and "assistants" and "privacy" or "surveillance". I also placed down a particular time period which was "since 2016", as that's when these assistants were widely used and criticized. The presentation of my secondary research will start out with a description of the working of a specific IT system, and then progress into supporting and discussing concerns with respect to my primary research results. The survey data will be represented in forms of pie charts and average number ratings to give a clear idea of what users' believe.

IT System

The term Virtual Assistant, is a smart software embedded in Smartphones and other connected devices that acts like a personal assistant by helping you mitigate your many tasks so that you can concentrate on the more important things(Samsung, a CTech Partner).

The list of skills a virtual assistant can perform grows each passing day.I will be focusing on, Amazon Alexa, the smart speaker, because it gives me room to explore the hardware required with it too, as Apple Siri is embedded into apple devices, however they work along similar concepts. (Khillar)

Starting off with the software, the heart and soul of this device is amazon cloud computing service called the Alexa voice service, it is a software-based service running on a lot of servers in one or more data centre, provided it is connected to the internet at all times. This cloud service is available to many third-party apps and developers in order to enhance and introduce new skills for Alexa to perform. It is Amazon/Google's responsibility to ensure the third-party servers authenticate the cloud. We argue that app developers often lack the security experience (Tripwire authors). As such, Amazon and Google, as the app store operators, are in the best position to act as the gatekeeper to ensure all the developer components that interact with their infrastructure (i.e., the cloud) are securely implemented The popularity of smart-home assistant systems such as Amazon Alexa and

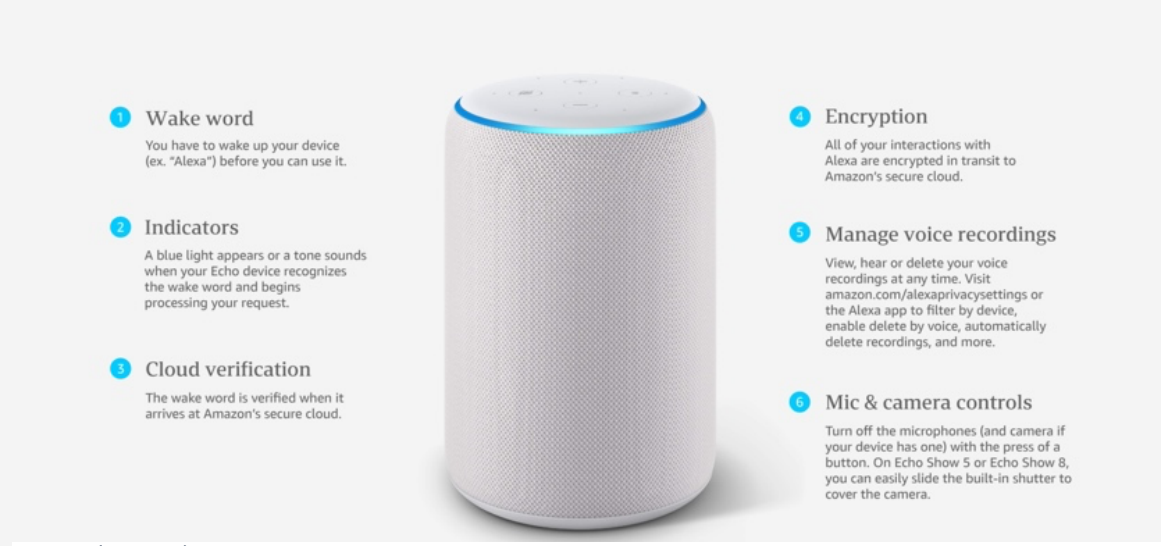


Figure 2 (Amazon)

Google Home leads to a booming third-party Application market (over 70,000 applications across the two stores). While existing works have revealed security issues in these systems (Hu et al.). These skills result in commands ranging from simple questions such as "what is the weather like today" to the device acting as a security device. When the customer says the word "Alexa", it acts as a wake-up call, then turns the indicator on which is a ring-like LED light on top of the device, that is when you can make sure Alexa is listening and also control the volume.

It is not just an assistant which converts voice to text. Firstly, the voice clip is sent over to the cloud, which has the ability to interpret it into a text/readable format, when it matches with the word “Alexa,” this method is called “keyword spotting” (Jose). Similarly, it deals with all other commands in the same way. This method collectively is called Automatic speech recognition, using patterns in waveforms, it resolves a sentence into its components parts and describes their syntax styles.

The hardware of Alexa is a cylindrical shaped body device which is about nine inches tall and a three-inch diameter. It has two buttons on top of it, one of them is to switch the microphone on and off. This gives you the choice to choose when you don’t want Alexa listening to you at all. The other button is an action button, to wake her up instantly. The 7-microphone array on top makes the working of Alexa so efficient, equipped with beamforming technology which means that it is allowed to send wireless signals towards a device and active noise cancellation to reduce the background and surrounding noises. It consists of three circuit boards with a NAND flash storage which is non-volatile, to transfer the voice recordings to data centres (Johnson)

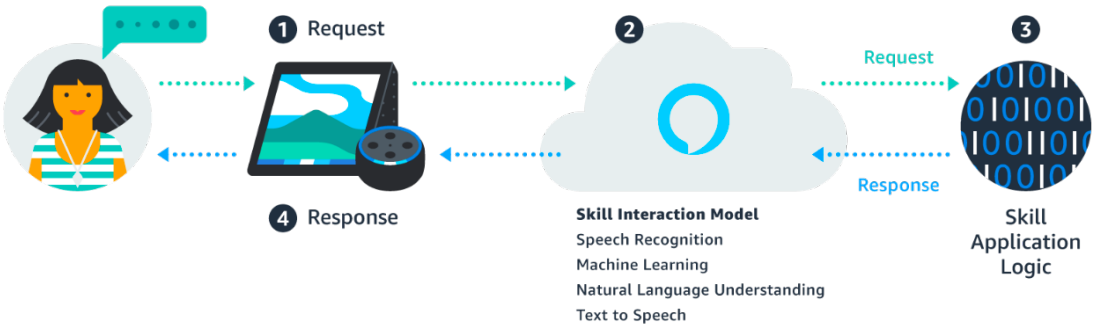


Figure 3 (Amazon)

In simple words, the input here is your voice recording asking for it to perform a specific task. The processing is done by the Alexa Voice Service. And the output is the results sent from the cloud service back to the device and Alexa says it out loud.

Literature Review

Research has been done om how these devices have caused concerns just because it is a device which “listens”. Boughman, Eric, et al believe that personal data of the user’s which the device has recorded by be sent to third parties. The question he raised is “Why are individuals ready to sacrifice privacy for convenience offered by digital assistants, will their profile become more akin to a private journal?” He believes that this is a sign of weak artificial intelligence, Current digital assistants are examples of “weak artificial intelligence.” which means that it can run only a specific amount of tasks, it is also referred as narrow because it enables some very robust applications. (IBM). Boughman, Eric, et al argument is that these recordings can reveal a lot more than we think from the user’s state of mind to physical characteristics. The biggest implications rise here, which is the data being used further in order to act as substantial evidence in court cases or it can be used by companies to strategize their public relations by selling it to third-party corporations. However, to argue on that Bezos, the former CEO of Amazon said his company is also embracing that kind of technology that would make it difficult for government officials to gain access to any personal information on its devices — even when those authorities have a warrant. Such measures prevent device-makers from accessing their own customers' data. He ensures that the company is adhering to its own privacy policies, which promises not to violate users' privacy and not use that information for advertising or surveillance (Tsukayama, Hayley) This assures the users but only to a certain extent. At the same time, the recorded data provides scope to the company to improve the skills of the Virtual Assistant and to make it more efficient in further updates, it is used as feedback for technical improvements. These sources have built a conflicted argument regarding the usage or the recording more than the reason for why is it being recorded and how is it secure. However, not much evident development has been noticed with this use of manual machine learning.

Social and Ethical Considerations

I would like to begin to define the two main social impacts and ethical considerations outlined ahead. Privacy and Anonymity, the ability of individuals and groups to determine for themselves when, how and to what extent information about themselves is shared with others. At its extreme, privacy becomes anonymity when for instance , a person uses it to conceal his or her true identity and misuse it. The idea of corporate surveillance is the use of IT and devices to monitor the actions of people. The key data tracking method discussed in this essay is with the use of sensors, that can capture voice recordings and videos and send them to remote Web services, extending the IoT footprint beyond the four walls of a home ("Digital Footprint").Data is stored in multiple forms and for multiple purposes in various Amazon services, such as S3 and DynamoDB. (Amazon) All information is treated with high confidentiality and we use multi-factor authentication to restrict access, service encryption and audits of our control environment to protect. (Day et al.) This sounds great to convince the users, yet in this context it is not enough.

Starting with the results of the first question regarding which virtual assistant do people use the most and for which skills, gave me an idea about the amount of data or information the

assistant holds of them. My interviewee's response was Google home because of the reasonable price and the attractive hardware. According to the survey, the majority was Apple's Siri with 41%.

Figure 4 (Personal Survey)

It is interesting because, firstly iPhones, iPads are widely used around, so it is a virtual assistant which is the most accessible because it is embedded into the device. So no additional purchase was required. Secondly , apple has built a sense of trust and loyalty amongst customers, by laying out their policies in simple words online. They respond to the obvious users' concerns and understandable even for a user who is not proficient in the use of

technology. The company has clearly stated that before we suspended grading, our process

Figure 5 (Personal Survey

involved reviewing a small sample of audio from Siri requests — less than 0.2 percent — and their computer-generated transcripts, to measure how well Siri was responding and to improve its reliability.

The contents of your messages aren't transmitted to Siri's servers, because that isn't necessary to fulfil your request ("Improving Siri's Privacy Protections"). These provide a sense of assurance to the customer's but also objects against the methods of machine learning other companies use. But I believe that the mention of 0.2%, does not worry the customers, because apple focuses on Siri's response more than your query. For this sole reason, apple stands true to their promises made regarding privacy to a certain extent. This brings me to the question about the End user license agreement, it is certainly long and detailed, which is very hard to understand. According to my survey, 81% of the respondents do not read the EULA, mainly for the reason of it being too long or they weren't aware of its

existence, which I feel is justifiable because users are to blindly trust certain devices because of the big companies they are developed by. Amazon has ranked first in the trust index and Apple received a similar value amongst other big tech companies in a survey where users were asked to rate their level of trust with major tech companies when it comes to protecting users' personal information (Seitz). I would like to talk about one interesting response from a user regarding not reading the EULA was “Too lengthy, it’s driven to protect the OEM vendors from copy rights infringement, privacy law.” My interviewee would also agree to this response, he believes that EULA are used to shield to protect the company from legal consequences but fail to do so morally and do not assure the customer that their data is in safe hands. Similarly, the interviewee spoke about an interesting approach to EULA agreements by making them interactive, in the sense the terms and conditions should pop up when and where they are relevant, such as deleting of data in a set of period. Interestingly there is an option to delete the voice recordings. But the company still has that data, just not as a sound bite. It keeps the text logs of the transcribed audio on its cloud servers, with no option for you to delete the data (NG).This clearly outlines this feature being namesake just to meet with certain laws. I then continued over to question the users about third party apps and skills, this question was raised when I came across this article about Alexa signing off with a night-time benediction (such as sweet dreams) after playing a night-time lullaby (Shulevitz). This is what made the user feel uncomfortable and have second thoughts about trusting the device. It sounds simple but however is alarming, which made the users think “Do I trust

you?", this is the reason third party companies are one of the primary stakeholders to consider.

This raised a question about invoking the wrong skill according to my survey it inclined to no. However the interviewee mentioned the difficulty his wife faces with the google home device, there have been instances, it defined the wrong word, mainly due to a different accent. The two columns in Figure are to distinguish between Amazon (left) and Google (right) which match my results.

Invoke a skill that did not intend to:		
Yes	29%	27%
No	71%	73%

Figure 6 ((Zhang et al. 5)

But, as the results are pretty similar for both the devices, the secondary data results don't support my technical reason, that google home doesn't use the authentication method between the cloud server and the input/output. However, Amazon Alexa uses a public-key based method. The cloud signs its request payload with a private key, and the skill endpoints can verify the signature using the cloud's public key when receiving the request. The verification is required. (Hu et al.) The other reasons for this could be the lack of context for

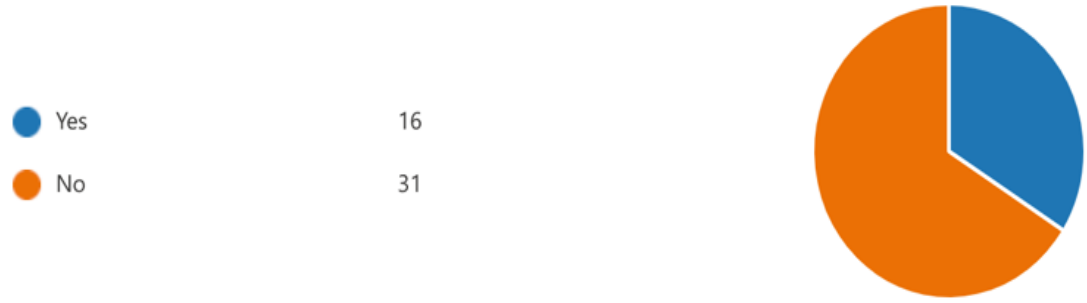
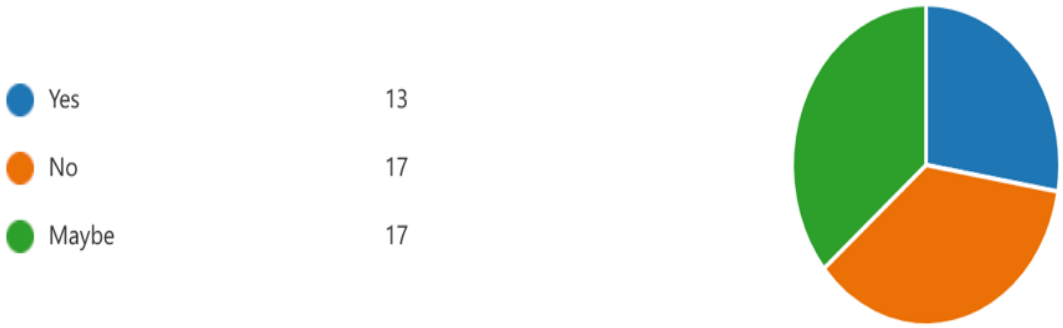


Figure 7 (Personal Survey)

the device or when the user does not use the device frequently, hence the devices isn't familiar enough with the respective voice. This shows that there aren't any major improvements in the functioning of the device. My survey also involved a straightforward

question," Is it invading your privacy?", this question surprisingly had equally disputed answers, yes (28%,) no (36%) and maybe (36%). However amongst my respondents 89% of them were aware that the device is listening to them, which makes it more interesting. However from another survey from a paper suggests the same, Intelligent Personal Assistants (IPAs) ,Some percent- age of users expressed that they do not have any privacy concerns but when they learned about the "always listening" feature of these devices, their concern about privacy increased to about 68.63% of users responded to the survey that they have concerns with regard to the privacy while utilizing Amazon Echo in their daily lives, however this data was from 51 university students earning a degree in the STEM branch. This shows that they were more aware about the privacy issues and further implications of their data being recorded such as the device getting hacked, the device storying personal information such as



credit card information and know the fact that Further, data collected by smart devices has made its way into the public domain, potentially compromising the security of those it belongs to (Turner).

However, the contrast in these results from my survey and the second survey is that the users believe that it creates a large positive impact in their daily lives, this means that the ease of having to say certain words to switch on a light or to get a word's definition overcomes the idea of their personal data being on the risk. This shows that the simple awareness of the real concerns can affect a large population's mindset towards something,

Figure 8 (Personal Survey)

users begin to restrict certain skills on the device. Many users expressed that they are aware of the privacy concerns and they do take actions: a) returning the product; b) muting the microphone; c) limiting the us- age – example only using to set alarms. (Zhang) However, this does not answer my question quite yet because, 68.63% of users responded to the survey that they have concerns with regard to the privacy while utilizing Amazon Echo in their daily lives. But my survey disagrees, as for the question "The comfort of using a voice assistant is worth risking your privacy. (1-strongly disagree 5-strongly agree), the average rating fell on 2.3 which is less than 50%. The interview also mentioned that he doesn't trust the device , however still utilise it, he believes that is the nature of technology.

Now that we have a good overview regarding the review of users and an expert.

Lastly, regarding the statement "It is justifiable that Companies listen to your voice recordings in order to enhance the functioning of their product. "(1-strongly disagree 5-strongly agree). The average rating was 2.51, which is little means that the user's can't argue much against that however it isn't a higher number because of the reason stated by my interviewee, he believes that it is a machine learning technique but he has not noticed a significant improvement in the function of his device. The effective solution he believes are opened source software such as almond which are ready to be used by enthusiasts to automate nontrivial tasks. Almond's open and learning infrastructure will hopefully attract enough contributions for it to grow to serve a more general audience over time.

Conclusion

We can consider the idea of shifting the burden, where these evolving virtual assistants provide a plethora of features leading to be the privacy predicaments for which the most valuable public companies are now questioned. Every minute that your virtual assistant is plugged in, adds data to your passive digital footprint. I believe that from the users' point of

view, it is inferred from the above analysis that they value leisure, ease of utilizing voice interface more than the plausible risks of their voice recordings being heard by more than just the device. However, from the point of the developer companies and the third party applications, they attempt to stick to a consequentialist point of view choosing to provide users with a better experience of automated tasks. However, it affects their moral decisions leading them into the debate of invading users' privacy. There is no shortage of changes that tech companies can make to improve user experience and safeguard our information, such as shorter and clearer privacy policies, more definitive opt-outs for location tracking, more regular destruction of aging or leftover user records, and more transparent disclosure of which third-party applications have access to our information. However, we're fundamentally willing to exchange some measure of privacy for great gobs of technology. We are reconsidering our prior assumptions and examining whether our society should recalibrate itself in favour of greater protection over user data. (Rosen) There lies an ulterior motive from the companies point of view, which in turn is proposed to users' as a way to enhance their daily life. However, if this issue persists, there is no limit to the future implications here. The growth of virtual assistants in more and more devices such as fridges and cars will be controversial, till methods of machine learning depend on human resources.

Works Cited

"Alexa Privacy and Data Handling Overview." AWSSTATIC, d1.awsstatic.com/
product-marketing/A4B/
White%20Paper%20-
%20Alexa%20Privacy%20and%20Data%20Handling%20Overview.pdf.

Accessed 10 Nov. 2021.

"Amazon Alexa Privacy." Amazon, www.amazon.com/Alexa-Privacy-Hub/b?ie=UTF8&node=19149155011#privacybydesign. Accessed 10 Nov. 2021 *Amazon*.

"What Is Automatic Speech Recognition? - Alexa Skills Kit Official Site." *Amazon (Alexa)*, 2021, developer.amazon.com/en-US/alexa/alexa-skills-kit/asr. Accessed 17 Sept. 2021.

Apple.

"Improving Siri's Privacy Protections." *Apple Newsroom (Singapore)*, 2019, www.apple.com/sg/newsroom/2019/08/improving-siris-privacy-protections/. Accessed 17 Sept. 2021.

Authors, Tripwire Guest. "AWS vs. Azure vs. Google – What's the Difference from a Cloud Security Standpoint?" *The State of Security*, 29 Dec. 2019, www.tripwire.com/state-of-security/topics/featured/. Accessed 26 Sept. 2021.

Boughman, Eric, et al. "'Alexa, Do You Have Rights?'" ["Business Law Today"]. *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, July 2017, pp. 1-5. *JSTOR*, www.jstor.org/stable/10.2307/90011461. Accessed 16 Feb. 2021.

Brewster, Thomas. "Amazon Argues Alexa Speech Protected By First Amendment In Murder Trial Fight." *Forbes*. *Forbes*, www.forbes.com/?sh=733496d72254. Accessed 17 sep 2021.

Brickner, Taryn. "Virtual assistants will power the future workforce." *Raconteur*, 18 june 2020, www.raconteur.net/. Accessed 26 Sept. 2021.

Day, Matt, et al. "Thousands of Amazon Workers Listen to Alexa Users' Conversations." Time. TIME, time.com/5568815/

amazon-workers-listen-to-alexa/. Accessed 10 Nov. 2021.

"Digital Footprint: What is it?" Packetlabs, packetlabs.net. Accessed 10 Nov. 2021.

Education, IBM Cloud. "Artificial Intelligence (AI) Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind." *IBM Cloud Learn Hub*, 3 june 2020, www.ibm.com/sg-en. Accessed 26 Sept. 2021.

"How Does Alexa Work?" *Amazon*, www.amazon.com. Accessed 26 Sept. 2021.

IRIBARREN, MADDIE. "Microsoft Releases Voice Assistant Usage Report, Finds Apple Siri And Google Assistant Tied at 36%, and 41% of Respondents Have Privacy Concerns." voicebot.ai, 28 Apr. 2019, voicebot.ai/2019/04/28/microsoft-releases-voice-assistant-usage-report-finds-apple-siri-and-google-assistant-tied-at-36-and-41-of-respondents-have-privacy-concerns/. Accessed 10 Nov. 2021.

Jang, Yeibeech. "Exploring User Interaction and Satisfaction with Virtual Personal Assistant Usage through Smart Speakers." *Exploring User Interaction and Satisfaction with Virtual Personal Assistant Usage through Smart Speakers*, aodr.org/xml/24999/24999.pdf. Accessed 16 Feb. 2021.

Johnson, Bernadette. "How Amazon Echo Works." *Howstuffworks.com*, 16 Nov. 2016, electronics.howstuffworks.com/gadgets/high-tech-gadgets/amazon-echo.htm. Accessed 16 Feb. 2021.

Jose, Christin, et al. "Accurate Detection of Wake Word Start and End Using a CNN." *arXiV*, 9 Aug. 2020. *arXiv*. Accessed 26 Sept. 2021.

Judith Shulevitz, Judith. "ALEXA, SHOULD WE TRUST YOU?" *The Atlantic*, Nov. 2018. *The Atlantic*, www.theatlantic.com/world/. Accessed 26 Sept. 2021.

Kesten, Gayle. "15 mind-blowing stats about voice assistants." *Adobe Blog*, 21 Sept. 2020, blog.adobe.com/. Accessed 6 Aug. 2021.

Khillar, Sagar. "Difference Between Alexa and Siri." Difference Between Similar Terms and Objects, 14 July, 2020, http://www.differencebetween.net/technology/difference-between-alexa-and-siri/.

Lavin, Andrew. "Ethical Dimensions." Andrew Lavin Portfolio and teaching resources, alav.in/teaching-resources/. Accessed 10 Nov. 2021.

Manikonda, Lydia, et al. What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants. 27 Dec. 2018. ACM, dl.acm.org/doi/10.1145/3278721.3278773. Accessed 26 Aug. 2021.

NG, Alfred. "Amazon Alexa transcripts live on, even after you delete voice records." CNET, 9 May 2019. CNET, cnet.com. Accessed 10 Nov. 2021.

Partner, Samsung. "What Is a Virtual Personal Assistant, and Why You Need One." *Ctech*, www.calcalistech.com/ctech/home/0,7340,L-5211,00.html. Accessed 26 Sept. 2021.

Prensky, Marc. Weblog post. *Digital Natives, Digital Immigrants*, Marc Prensky, 2001, marcprensky.com/writing/default.asp. Accessed 25 Sept. 2021.

Rosen, Michael M. "Why We Choose Surveillance Capitalism." *The Center for the Study of Technology and Society*. *JSTOR*. Accessed 27 july 2021.

Security Vetting Process of Smart-home Assistant Applications: A First Look and Case Studies. 13 Jan. 2020. *arXiv*, arxiv.org/pdf/2001.04520.pdf. Accessed 29 Apr. 2021.

Seitz, Patrick. "Survey Reveals Which Tech Companies Consumers Trust The Most." *Investor's Business Daily* [California], 2 Aug. 2021. *Investors Business Daily*, www.investors.com/news/technology/tech-stocks-survey-reveals-which-tech-companies-consumers-trust-the-most/. Accessed 26 Sept. 2021.

Sui, Sylvia. "State v. Bates: Amazon Argues that the First Amendment Protects Its Alexa Voice Service." *Harvard Journal of Law and Technology*, 25 Mar. 2017, jolt.law.harvard.edu/digest. Accessed 26 Sept. 2021.

Tsukayama, Hayley. "Amazon CEO Jeffrey Bezos: Debate between privacy and security is 'issue of our age.'" *The Washington Post*, 19 may 2016. *The Washington Post*, www.washingtonpost.com/news/the-switch/wp/2016/05/18/amazon-ceo-jeffrey-bezos-debate-between-privacy-and-security-is-issue-of-our-age/. Accessed 16 Feb. 2021.

Turner, Lance. "House that think." *Alternative Technology Association*. *JSTOR*, www.jstor.org/stable/10.2307/90022942. Accessed 27 Sept. 2021.

Wang, Qian Emily, et al. "Digital Natives and Digital Immigrants." BISE.

BISE, www.bise-journal.com/?page_id=18. Accessed 10 Nov. 2021.

Zhang, Nan, et al. *Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home*. 3 may 2018. *Cornell University*. Accessed 17 Sept. 2021.

Zuboff, Shoshana. "The Defintion." Introduction. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, e-book ed., New York City, PublicAffairs, 2020.

Appendix

Expert Interview Transcript

1. Which virtual voice assistant do you greatly?

Google home devices mostly, 90%, I do have an iPad, so Siri occasionally however I do find it annoying.

2. Is there any reason for choosing this device and not amazon Alexa or apple home pod?

Looking at the hardware devices, don't use virtual assistants on phones, I don't know why they have it, a digital immigrant, so it was a small one, and I wanted to have a play with it. It was also cheaper, and amazon has more implications when it comes to selling adverts, I use the amazon website to buy stuff, so google had other elements to it. Got one free too, bought the bigger models. I do have 6 setups around my house and the fans too. You could say to turn the fan on and off, etc.

3. What do you usually use it for?

That’s interesting, when I got it, it was for the time, jokes, spotify and youtube, I have linked the accounts, for music mainly, searches and definitions, listening to podcasts, games initially with my daughter and story telling. I had it also connected veemo lights, and basically in every room connected to the light switch

4. What is the Wake word? Are there any False positives?

Okay google is what I used, not sure if I can change it, I tried but I couldn’t. Because the way you set it up, it answers whenever you ask it *demonstrates by asking the time* and mistakes clarity of conversation sometimes, it does say "I don’t understand what you said" during a discussion randomly.

5. Have you ever invoked a wrong skill?

It doesn’t understand, possibly because it needs understanding and context of the conversation, and it is used to my voice I have trained it, not with wife and daughter. Sometimes with my wife's accent, it doesn’t understand it, or it defines the wrong word sometimes.

6. Biggest problem you have faced?

I am a privacy advocate, sold my soul for some reason, it is interesting to understand why. However, I have got only one google home set up but I hardly use it now. It feels more like a gimmick with my age, I’d rather type something in. I used it for music mainly, I do worry about my data and information to some extent. One good thing is I can clear my history, google maps, search, and assistant. And you can look back to what you said and asked. As a ITGS teacher, I do forget about it too sometimes, when other people are over, and you ask it to

play something, that is a great thing. I prefer an assistant which wouldn't save everything, so why do then have to do it. I have paid the money, so it feels like a business advert.

7. How do you know whether a skill has stopped?

The small one does have a little shiny light, it isn't very apparent , however the mute button is there on one side, but it isn't easy to press it or enable it like the other buttons, cant suddenly do it. I can't say it. Tap it to come back on. The interface is not through voice or physically easy I would say.

8. Will this affect how you use your device in your day to day life now?

I know it is always listening and I still do have it on, in bedrooms, bathrooms, lounge and the kitchen. What I am getting back from it in the long term, there are other opportunities, using duck duck go as a browser or the VPN, there are many alternatives to protect my privacy. Similarly, I am waiting for this field to do the same. And I would move over to the system which would do the same, ensuring my privacy.

9. From a computer science teacher's perspective, what are your thoughts on personal voice assistants and user privacy?

I don't know really, I wonder if it's just 3d cinema a gimmick, unless the technology advances and becomes more integrated, I probably will still be continuing using it.

Depending on development, what can they do, sometimes talk to other devices and third-party apps, interoperability lack of it, Getting them working, easy for me, but user friendly na, protocol? Stops working suddenly development of smaller companies with open source

ones, the ones who don't use your data, do we really need the data? I am not buying anything new until they have improved massively.

Ethically, things have changed a lot in my time in some ways, but computers are the same. But the use of technology has risen exponentially, autonomous cars legally will happen eventually, I would love to use it. Vice interfaces are just natural now.

10. Consumers have lost all control over how personal information is collected and used by companies. (Do you agree?)

100%, agree, we have no control, methods and means that can be put into place, the ability that your data disappears after some time, we could code it, like snapchat it disappears, that can be done in other aspects. But companies won't do it cause it costs money. Govt intervention and privacy advocates need a approach the companies can utility.

11. Most businesses handle the personal information they collect about consumers in a proper and confidential way (Do you agree?)

No, your data is a way to make money, how many do I trust? Very few? Security issues don't have the expertise even the bigger companies to properly securely info we volunteer give them. Large number of leaks happening in a day, about 1000s, they do say it is encrypted but I don't trust it.

12. Should companies access your recordings to improve and enhance the device's skills?

I can see it why, that is how machine learning works, it captures all the data, getting humans to improve its abilities. But I haven't seen much improvement or change while conversing with me. Especially when my daughter and wife use it, so it sets limitations, you remember

only few skills which it could do, you stop being fluid about it, you stop trying things you just give up with the I don't understand. Early on I used to search about the latest keywords and skills it could do, jokes and stories but I am passed that. So the voice interface compared to a text interface, I am prepared to explore, but here I feel stuck or trapped when I'm researching.

13. EULA, thoughts?

I got no time, it is more precious, no I haven't gone through it, I feel like they are set up to be not read by anyone, cause its so tough, I don't know the solution to it, the complexity is high, there should be a simplified version of it, and then you could read more to know the complex part about it. It is a 30 page document maybe, and no one can read that, it is for all the products now, not suitable for human consumption. It is hard to deal with it.

No, it is like writing a document in a different language, they know why they do it, maybe bullet points, main issues to what you are agreeing to, companies have not gone half way, it can be used legally to get away but morally no I wouldn't say so. So the government intervention needed, the EULA can be long but also writing simplified, main things what you are agreeing to. Apple have started to do it to accept permissions when it comes to media, photos.

Maybe it has to be interactive, simplification, doing something for me, in a sensible approachable way, delete my data in 90 days.

14. Is it okay if your recording can be used in Court cases?

No of course not, you don't know how the evidence is interpreted, it is only one form of it, in my private home and domain. But difficult to argue, it has been used in murder cases, and

the noises have been part of it to convict someone, well it isn't a good use of the technology but the problem I suppose goes to solving a murder and in Thailand, a stricter government when it comes to the king, so it isn't fine, it can get me into trouble. Singapore wouldn't use it cause there are many issues, but in china the manpower yes. So similar to Facial recognition technology, dog poo in the grass, they still use it for that, the creep of the use was tangible, and now you are under surveillance state technically.

15. On a scale of 1-10? How much do you trust it?

I trust it 0 but I still utilize it, that is the nature of technology at the moment, willing to sell our control, how much ever know we know what's happening, I know a lot but yeah I will still use it.

Survey Questionnaire

The use of virtual assistants

The answers are anonymous, please read the questions properly as this is for my Extended Essay. Please contact ---------in case you want to withdraw your answers.

1.How old are you?

2.Which virtual assistant/s do you use the most?

Amazon Alexa

Apple's Siri/ Homepod

Google home/assistant

Other

3.How many third party apps/skills have you linked to your virtual assistant? Which ones?

4.Do you trust the device with your personal information

Yes

No

It depends

5.If you chose no or it depends, please elaborate

6. Please name two skills that you use most often. (Eg. To set a reminder, To stream music, etc.)

7.Does the device influence your life positively?

Yes

No

Maybe

8.Do you think it is invading your privacy?

Yes

No

Maybe

9.Are you aware that some of the devices might be always listening and recording?

Yes

No

Maybe

10.Would you mute the microphone if you have an option to ?

Yes

No

Maybe

11.If yes or maybe, why?

12.Do you know how to view your voice history

Yes

No

13.Would you delete it, if possible?

14.What wake word do you use ?

15.Does the device wake up when you do not want it to?

Yes

No

16.Is there an indicator to know when it is listening to you?

Yes

No

Not aware

17.Have you invoked a skill you did not intend to?

Yes

No

18.Have you read the End User licence agreement?

Yes

No

19.If no, why not?

20.Consumers have lost all control over how personal information is collected and used by companies (1-strongly disagree 5-strongly agree)

21.Most businesses handle the personal information they collect about consumers in a proper and confidential way. (1-strongly disagree 5-strongly agree)

22.Existing laws and organizational practices provide a reasonable level of protection for consumer privacy (1-strongly disagree 5-strongly agree)

23.It is justifiable that Companies listen to your voice recordings in order to enhance the functioning of their product. (1-strongly disagree 5-strongly agree)

24.The comfort of using a voice assistant is worth risking your privacy. (1-strongly disagree 5-strongly agree)

25.On a scale of 1-5, how much do you trust your device? (1 is least, 5 the most)