Home Automation Systems: A Recommendation Report

Prepared for: Mrs. Inge Fink

Prepared By: David Pace

April 13, 2020

Table of Contents

Table of Contents ……..……..…..... 2

Executive Summary ……..…….…… 3

1. Introduction ……..……..... 4

2. Research Methods …….…….…….…….. 4

3. Results …….……..……. 4

3.1. Affordability ……...…….……. 4

3.2. Security/Privacy……..……..……... 6

3.3. Capabilities……..…….…….……..... 7

4. Conclusions ……..……..… 8

5. Recommendation ……..…… 9

Works Cited ……..…….. 10

Executive Summary

Home automation systems have been an expanding industry over the years, and consumers have been left without an idea on which system is ideal. I looked at three of the top companies in the market - Amazon, Google, and Apple – and compared them by their affordability, security/privacy, and capabilities. My research used the three companies' websites, online articles, and academic resources. The conclusion indicated that Amazon is the most affordable option with the most available products and diversity, but it is not extremely private and secure. Google has the smartest technology available, but they do not have a lot of home accessory products and they lack diversity. Google's pricing is slightly more costly compared to Amazon, but they share the same level of security and privacy. As for Apple, it costs just as much as going with Google, but they have a larger amount of general and unique products available. Apple also has the most secure and private home automation system; they do not collect a bunch of personal data about their users and any data that is stored is encrypted and stored locally on the Apple device. If you are looking to start purchasing smart home products at the lowest prices available, want a large variety of options, and are not concerned about what information is collected about you - than Amazon's home automation environment is the best for you. If you want a system that's a little smarter and are willing to make the sacrifice of having less variety, go with Google. Finally, if privacy is a concern, then Apple is the choice.

1. Introduction

My recommendation report identifies which home automation system services are the best for users out of the three major, technological giants: Amazon, Google, and Apple. The home automation environment is powered by a central hub. The central hub's job is to connect different appliances, sensors, and applications to the internet through artificial intelligence (AI) API or software. According to Isa and Sklavos, computer engineering researchers at the University of Patras in Greece, every home automation system has a central hub unit or simply put, the brains of the system, that allows connectivity (2). Central hubs are better known as smart speakers, displays, or any device with AI software. Each company has their own version of AI software: Amazon's Alexa, Google's Assistant, and Apple's Siri. Because the best system is subjective to the desires of the user, my recommendation focuses on three basic criteria that every home automation system should have: affordability, security/privacy, and capability.

2. Research Methods

I conducted research using information found at each corresponding company's website, online articles, and the Academic Search database; provided by UNO's online, library resources. I used the information I gathered through research about home automation systems in order to subject them to different levels of analysis. The most intricate level, security/privacy, relies on academic research and specific case studies. Other levels of analysis, such as affordability and capability, resort to raw, objective data collected from their respective companies and from journalists.

3. Results

3.1 Affordability

In order to completely assess the cost of a home automation system with Amazon, Google, and Apple. The affordability criteria will explore price ranges of the available central hubs and the costs of certain types of accessories. Since no two accessories are identical, the overall price significance of different categories will be used to determine the ultimate affordability of each company. The significance of these different prices lies in the details, but the most important aspect of this criteria is how low of a cost users can get away with.

Amazon offers an array of different central hub smart devices and accessories for home automation. The price ranges, in dollars, are derived from Amazon's website. Amazon appears to have the largest number of accessories for the most diverse prices. If a user is looking to find cheap home automation accessories, Amazon offers the best budgeting.

Amazon Affordability	
Product Type	Price Range
Central Hubs	$50 to $230
Lighting	$6 to $1080
Locks	$10 to $437
Cameras	$16 to $649
Sensors	$13 to $400

Google offers several central hub devices, but when it comes to accessories, the available products are limited. The price ranges are derived from Google's website. Any singular price tags are due to limitations of the quantity of products for that category. Google tends to be costly and it lacks cheap alternatives and varity to certain products.

Google Affordability	
Product Type	Price Range
Central Hubs	$30 to $300
Lighting	$30
Locks	$279
Cameras	$200 to $400
Sensors	$120 to $400

Apple only offers a single central hub device, and it offers a decent amount of home automation accessories. These prices can be found on Apple's website. The available products are not super diverse, but there are some unique options available. Apple also tends to be costly, but it does have some cheap alternatives to certain products.

Apple Affordability	
Product Type	Price Range
Central Hubs	$300
Lighting	$20 to $200
Locks	$200 to $230
Cameras	$40 to $600
Sensors	$40 to $100

3.2 Security/Privacy

Amazon's Alexa has had some concerning mishaps in the past. There was one peculiar occasion, publicized by Tom Warren, senior editor for The Verge, where the API recorded a conversation between a husband and his spouse and sent it directly to one of his employees (2). This particular event may be a bizarre scenario, but in an article on Bloomberg, "Amazon Workers Are Listening to What You Tell Alexa," it is confirmed that Amazon's employees regularly listen to the recordings that Alexa collects from its users (Day, et al. n.p.). Due to the situation where a private conversation was sent to the user's associate, whose to say that this is not a habitual thing that occurs with Amazon's Alexa. The likely hood that Alexa monitors users unknowingly seems increasingly so, and Kevin Webb writes about lawsuits that have been brought against Amazon in several states in his article, "Amazon just got hit with a lawsuit that claims it's putting children's privacy at risk by recording what they say to Alexa" for Business Insider. One lawsuit in particular is concerned about the privacy of children being violated (1). In response, Amazon has taken measures to allow users to delete past recordings of themselves and toggle whether to collect future recordings (Webb 6).

During the COVID-19 pandemic, Greg Kumparak wrote an article for Tech Crunch, "Google is lowering Nest camera quality 'to conserve internet resources'," that covered an email Google sent to its users. Google made the decision to modify the bandwidth that their Nest Cams use in order to preserve resources during the pandemic (n.p.). They did this by limiting the video recording quality of these cameras remotely. This is only possible due to the IoT (Internet of Things). The overall objective of the IoT is to allow users to access and control objects such as

Google's Nest Cams from any place through the internet. According to Ali, Bako, and Ali Ismail Awad, researchers at Lulea University of Technology, in their article "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes" the authors demonstrate how the IoT reveals many more opportunities for a hacker to remotely exploit a vulnerability in software. A hacker using a network attack may try to, "intercept, manipulate, fabricate, or interrupt the transmitted data" (Bako et al. 5). It's even more disconcerting that Google can manipulate the cameras they sell, despite not having physical – local - contact with them. In fact, Google's unprecedented control of their Nest Cams imply that they have just as much or more control over these devices than the consumer, and the latter is more likely. Tyler Clifford from CNBC news reports, "Google must sway Congress on regulations or tech will face 'direct threat,' says cybersecurity expert." Google's unprecedented control gives some insight as to why they have been pressed by Congress about privacy concerns in recent years (n.p.).

Apple has been a longstanding role model when it comes to the information they collect about their users and how it is actually used. On their website, Apple claims that it collects much less data than other big tech companies and in order to maintain discretion, they randomize data in a way that makes it impossible to identify the source of it. According to Jon Porter, et al. in their article for Tech Radar, "Amazon Echo vs Apple HomePod vs Google Home: the battle of the smart speakers," data on an Apple device is encrypted to obfuscate your personal information and is saved locally on the device itself and is never sent to be saved over an online network (n.p.). Jefferson Graham, tech columnist, confirms this claim, but provides a bit more insight on his article for USA Today, "Is Apple really better about privacy? Here's what we found out." Generally, only in certain situations does Apple require information from its users. Such as the device's location in order to provide services like GPS (Global Positioning System). These types of requests are very few and far between an are never sent outside of the company or saved in some database after (Graham para. 10). Although Apple may not directly keep information about its users stored in a cloud, users can still choose to share information with other companies, and in most cases, other companies will store it.

3.3 Capability

Amazon, Google, and Apple all have their own respective specialties in regard to their capabilities. The capability criteria will be defined by the ability of the artificial intelligence APIs and home automation technology provided by our options.

Amazon's Alexa has been developing for about six years now. It is an impressive voice-controlled API. Over the course of time, Alexa has grown from being limited to primitive commands to being able to understand different iterations of the same question (Porter, et al. n.p.). This gives users the ability to voice control hundreds of home automation devices on the

market that are compatible with Alexa. Any compatible devices will link to Alexa through the IoT and be controlled under a profile. Profiles are a feature that allows different household members to be identified differently by Alexa. It's possible to switch between profiles on a device by requesting Alexa to change it for you manually. Many of the available home automation devices are owed to Amazon's partnerships with third-party companies. One of the most notable of these third-party companies is Zigbee, a workhorse in the IoT industry. It's also entirely possible to communicate with Alexa through Android and Apple devices, but it will require Amazon's Alexa app. Otherwise, users have the option of communicating with Alexa using an Echo device. The only downside is that the echo device is limited to its vicinity.

Google has been working with information parsing for over two decades (Porter, et al. n.p.). Google's Assistant is an impressive software, all the information Google obtained over the decades comes to life through the easily interactable voice-controlled API. Asking Google's Assistant a question or commanding it to do something feels incredibly natural in the sense that you do not have to follow strict doctrines (Porter, et al. n.p.). Google provides a profile system and automatically switches between profiles depending on whose voice it detects. When it comes to the home automation accessories, Google provides a surprisingly small number of products. They offer the bare minimum - lighting, cameras, and an alarm system. All of Google's home automation accessories can be controlled from an Apple or Android cellphone, so you do not need to purchase a central hub in order to interact with them as the cellphone can act in its place.

Apple has been working on Siri for a while, but because of their approach to privacy, they do not collect near as much information about how the API is used. This approach may keep your information safe, but it sacrifices the ability of Siri in-turn. Asking Siri questions is very limited, often times the API will resort to running a web search instead of having the answers on hand. The other noteworthy thing about Apple is how restrictive they are. Apple does not provide any third-party software access, so its limited to in-house services. For example, you cannot listen to anything but Apple Music by request from Siri (Porter, et al. n.p.). Because Apple does not allow portability between any other company, it becomes troublesome if you already purchased home automation products from other companies. Despite not being portable with other brands, Apple does offer a fairly decent amount of home automation products in their Home Kit. There are some unique products, such as water sprinklers, and some variety, such as different forms of lighting. Of course they also offer the necessities such as smoke sensors, locks, and cameras.

4. Conclusions

When it comes to affordability, Amazon offers the most products at the cheapest prices and has the largest variety when compared to Google and Apple. That's a huge deal, it's possible to get budget smart home products at Amazon while with Google or Apple your stuck purchasing $20-$30 light bulbs. Amazon clearly proves itself to be more affordable than Google and Apple,

but it's hard to find major differences when it comes to the cost of Google and Apple products. They're about the same in pricing but Apple has a larger set of products to choose from.

When it comes to the privacy and security of our options, Apple obviously is the most secure. Google has an appalling level of access to personal devices and Amazon spies on children, but Apple is the white knight in shining armor when it comes to protecting their users' privacy.

When it comes to the capabilities of our options, Google is the intellectual of the group. The API of Google's Assistant is unmatched, Amazon's Alexa comes at a close second, and Apple's Siri is very mundane putting it in last. In terms of portability, Amazon and Google are compatible with any Apple or Android, and they both have plenty of third-party company products they work with. This is the largest shortcoming of Apple - its seclusion from other companies - everything is done in-house; you cannot use Apple accessories without an IOS device. So to sum it up, Google is the smartest in terms of API, and Amazon has the better home automation environment. Apple's home environment is slightly more diverse than Googles, but it has portability concerns and it's not nearly as intelligent.

5. Recommendation

The best home automation system relies on a couple of factors: affordability, security/privacy, and capability. If you are looking to start purchasing smart home products at the lowest prices available, want a large variety of options, and are not concerned about what information is collected about you - than Amazon's home automation environment is the best for you. If you want a system that's a little smarter and are willing to make the sacrifice of having less variety, go with Google. Finally, if privacy is a concern, then Apple is the choice.

Works Cited

Ali, Bako, and Ali Ismail Awad. "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes." Sensors, vol. 18, no. 3, pp. 109–111 http://web.a.ebscohost.com.ezproxy.uno.edu/ehost/pdfviewer/pdfviewer?vid=3&sid=aa19842c-297e-4ab8-b21f-de408c70eb8a%40sessionmgr4008. Accessed 18 March 2020.

Clifford, Tyler. "Google must sway Congress on regulations or tech will face 'direct threat,' says cybersecurity expert." *CNBC*, 11 Dec. 2018, https://www.cnbc.com/2018/12/11/google-must-sway-congress-on-privacy-or-face-threat-cyber-expert.html. Accessed 18 March 2020.

Day, Matt, et al. "Amazon Workers Are Listening to What You Tell Alexa." *Bloomberg*, 10 April 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio. Accessed 18 March 2020.

Graham, Jefferson. "Is Apple really better about privacy? Here's what we found out." *USA Today,* 17 Apr. 2018, https://www.usatoday.com/story/tech/talkingtech/2018/04/17/apple-make-simpler-download-your-privacy-data-year/521786002. Accessed 18 March 2020.

Isa, E., and N. Sklavos. "Smart Home Automation: GSM Security System Design & Implementation." *Journal of Engineering Science & Technology Review*, vol. 10, no. 3, May 2017, pp. 170–174. *EBSCOhost*, doi:10.25103/jestr.103.22.

http://web.a.ebscohost.com.ezproxy.uno.edu/ehost/pdfviewer/pdfviewer?vid=6&sid=aa19842c-297e-4ab8-b21f-de408c70eb8a%40sessionmgr4008. Accessed 18 March 2020.

Kumparak, Greg. "Google is lowering Nest camera quality 'to conserve internet resources'" *Techcrunch*, 14 April 2020, https://techcrunch.com/2020/04/14/google-is-lowering-nest-camera-quality-to-conserve-internet-resources/. Accessed 18 March 2020.

Porter, Jon, et al. "Amazon Echo vs Apple HomePod vs Google Home: the battle of the smart speakers." *Techradar,* 25 Sept. 2019, https://www.techradar.com/news/amazon-echo-vs-homepod-vs-google-home-the-battle-of-the-smart-speakers. Accessed 8 March 2020.

Warren, Tom. "Amazon explains how Alexa recorded a private conversation and sent it to another user." *The Verge,* 24 Mar. 2018, https://www.theverge.com /2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation. Accessed 18 March 2020.

Webb, Kevin. "Amazon just got hit with a lawsuit that claims it's putting children's privacy at risk by recording what they say to Alexa." *Buisness Insider,* 12 Jun. 2019, https://www.businessinsider.com/amazon-accused-of-violating-child-privacy-laws-alexa-recordings-lawsuit-2019-6. Accessed 18 March 2020.