HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

Home Assistant Technology 13th March 2020 POSTNOTE

Figure 1 [i]

CANDIDATE NUMBER: 2004495

Overview

- **Enforced and mandatory regulations regarding cyber security is needed.**
- **These technologies pose threats to consumers personal data, physical space and emotional wellbeing.**
- **This technology needs to be governed by the state rather than technology companies – universal standards should apply.**
- **These technologies can connect together through the internet. Thus, they can all be hacked simultaneously.**
- **Increased governance over these devices will increase the economic benefits of these products.**

The gap between the real world and the digital world is shrinking[ii]. It's becoming increasingly harder to 'unplug' from the online world as everyday life, especially the home has become increasingly infused with technology[iii].Home assistant technologies are internet enabled devices that help consumers to keep control of their homes and lives at the click of a button. Van der Meulen estimates that by 2020 there will be 20 billion internet connected devices in the world and 12 billion of these devices could be used globally by consumers[iv]. These devices offer improved qualities of life to consumers, thus there is a growing demand for home automation through these products[v]. However, a change is needed regarding the security and privacy of these devices in order for them to reach their full potential and have optimal trust from the consumer. This brief offers an overview of home assistant technology and the potential dangers of this move towards a more automated life.

Background

These devices use artificial intelligence technology to collect your data and adapt to your lifestyle. The definition of smart home technologies has changed since the early development nearly half a century ago[vi]. This is due to the increased functionality of these devices. The internet connection and thus remote-control operation of these devices has allowed the capabilities of these devices to dramatically increase [vii]. Internet connected devices are often referred to as 'the internet of things' (IOT)[viii].The 1990s produced the early stages of what we now know as the IOT[ix]. The term 'home assistant technology' can be seen as an umbrella term used for a multitude of these IOT products. One of these products is voice assistant software. These devices perform task through voice recognition[x].Home assistants aren't just limited to voice-controlled devices this term also includes products such as smart thermostats and the ring doorbell. These products sync up to your phone so you can monitor your home on the go. The more data these devices collect the more powerful they become, this is due to their artificial intelligence and machine learning foundations[xi]. Amazon may be the market leader, selling 20 million devices last year. However other companies such as google are starting to catch up[xii]. This due to the increase demand for these products. By 2025 home assistant technologies are expected to have a global economic impact of over £11 billion[xiii]. While these devices provide both economic and social benefits they can also pose as a threat to people's personal cyber security.

The increasing demand and sophistication of these products however pose the issue of privacy. The online network that these devices use can also compromise the consumers privacy and security. They could be hijacked by hackers, disrupting and even taking over the consumers connection with these devices. The UK government however have a strategy put in place. By 2021 they hope to make

most new internet using devices and services cyber secure. They have even pledged £1.9billion to help tackle the cyber security of these products[xiv]. These products collect meta data and record anything from conversations to videos. They can even record patterns in the consumers everyday life. These devices can produce detailed picture of what the consumers everyday life may look like[xv].

Types of home assistant technology

- Smart fridge/ Fridge cam – This are connected to the cloud. It can connect to your phone and tell you when you are running out of certain foods. You can also send notes to your fridge from your phone. The fridge cam allows you to see what is inside on your phone.[xvi]There have been concerns that viruses could attack these fridges, causing the doors to open randomly. Neagle[xvii] notes that hackers can steal your personal details such as email data from these smart fridges.
- Amazon Echo- This is an Artificial Intelligence powered voice assistant that can connect to other smart devices in your house such as the locks and lights. It can control all these IoTs.[xviii].
- Smart lights -These are lights that can be turned on and off from an app or device such as the amazon echo[xix].
- Ring doorbell – This allows you to speak to the person at your door without opening it. It also records who comes up to the door, this data can be sent to your phone[xx].
- Smart locks- These locks can be controlled by devices such as Amazon Echo' and applications on mobile phones, using the internet. [xxi]

All home assistant technology uses the internet to connect to other devices such as a smart phone. They also use the internet to store data and provide extra services such as email and messaging.

Case study 1[xxii] highlights how IOT technologies can put the users at risk. Over time this sensitive, personal data stored as meta data in the cloud can create a detailed profile of the user. Hackers could even monitor this data to go on to also break into people's houses. They could monitor the smart lights in a user's house. If the lights have been off for a long time the hacker could assume that the user is not in the house hence, making it a prime target for burglaries. Thus, threats to online data can turn unto or facilitate real life threats.

Case Study 1

Strava- A fitness app exposed secret US army bases. The military users used wearable technology that linked to the Strava app to track their progress. Strava used the data collected to make a virtual map of where the military users ran.[1] This online map exposed sensitive military information.

Current regulations

There are no current standards for cyber security regulation of consumer products[xxiii]. Thus, manufacturers don't have to worry about and put money into the cyber security of these devices. This poses the question; How likely and easy is it to take control of these products?

Currently it is up to the individual companies to implement security measures within their devices. There is a lot of uncertainty around which laws companies need to abide by. This is due to the constant developments with the technologies being produced and the evolving threats.

The department of Digital Culture, Media and Sports proposed a voluntary code of practice in 2018[xxiv]. This was to try and help ensure that devices had strong built in security protection. However, this is not an enforced rule and is voluntary thus does very little to help with the issue of security.

The issues

In 2017 it was highlighted by academic researchers that there was a very real possibility that hackers could control smart lightbulbs[xxv]. Thus, it is important for governments to keep up with the rapidly changing environment created by technological advances. As these advances in the digital environment increase so do advancements in the ways people can hack into these IOTs.

A key challenge that needs to be addressed within home assistant technology is security features. As

there are currently no enforced rules or mandatory requirements regarding security practices[xxvi] with these devices, companies aren't funding ways to make them more secure. This is a key issue as most of these technologies use the internet and online networks, thus making them an easy and prime target. This weakness leaves consumers open to data theft. Increasing security within these technologies would also help increase consumer trust. This could help increase the economic benefits of this industry as more people would feel comfortable buying, using and integrating these technologies into their homes.

Data makes these technologies valuable. As more data is collected by these technologies, they can become increasingly more personalised and tailor your experience. This data is also useful to third party companies who could use this data to advertise products to the user. This data, however, can be used to create an invasive profile of the users. This brings about concerns of tracking, surveillance and once again privacy. These products often collect data without the users informed consent or knowledge[xxvii]. If a hacker was in control of a home's smart locks then the users physical space as well as digital space are both being compromised[xxviii]. Oulasvirta[xxix] emphasizes that not only are there threats to people and physical spaces but also their emotional wellbeing.

Hackers often use basic techniques to get into these devices. Trying common or default passwords is one of the main way's hackers take control of these devices.[xxx] Software vulnerabilities and programming errors are also a basic way in for hackers [xxxi] These technologies can connect together through the internet. Thus, they can all be hacked simultaneously. Figure 1[xxxii] depicts how through hacking the Alexa, criminals can affect the whole house if the target has multiple home assistant technologies. It depicts the device being hacked through voice commands.

Causes of poor cyber security

Economic factors often cause cyber security issues within commercial goods. Such as Insufficient funds and incentives being put into researching and creating proper security features.[xxxiii] Poor cyber security is not always down to the manufacturers. Cyber security also falls onto the consumer[xxxiv]. It is important that consumers use strong passwords that aren't repeated from other devices.

Future recommendations

Block chain stops any data being sent to the cloud.[xxxv]Most data leaks and hacks are targeted at the cloud as it is connected to the internet and thus an easy target. Block chain would allow for the data to not ever leave the users home, thus meaning no third-party companies could also have access to the data. Block chains is simply chains of data with no central authority[xxxvi]. No one can change or intercept the chains once they are added. It Users could have confidence that their data was safe and protected. This would also increase consumer confidence and thus have positive economic effects.

This technology needs to be governed by the state rather than technology companies. universal standards should apply to all home assistant technologies as they can sync together. This would put pressure on companies to fund and look into making their products

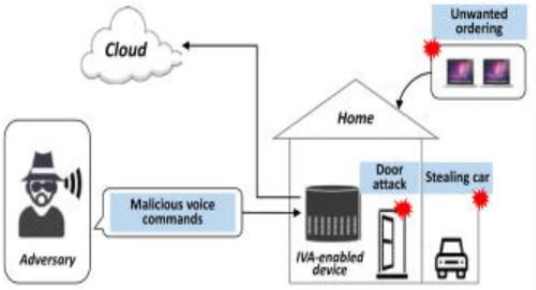

Figure 2

[i] Quartz. n.d. *What Our Tech Habits Reveal About The Future Of Smart Homes*. [online] Available at: <https://qz.com/1482503/what-our-tech-habits-reveal-about-the-future-of-smart-homes/> [Accessed 12 March 2020].

[ii] Chu, W., Chao, H. and Yang, S., 2016. *Intelligent Systems And Applications. Proceedings Of The International Computer Symposium (ICS) Held At Taichung, Taiwan, December 12-14, 2014*

[iii] Kitchin, R., & Dodge, M. (2001) Code/Space: Software and everyday life. MIT Press (opening chapter at: https://mitpress.mit.edu/sites/default/files/titles/content/9780262042482_sch_0001.pdf)

[iv] Van Der Meulen, R., 2017. *Gartner Says 8.4 Billion Connected "Things" Will Be In Use In 2017, Up 31 Percent From 2016*. [online] Gartner. Available at: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07 [Accessed 11 March 2020].

[v] Smart Home Automation using IoT& Virtual Assistant Dr. Bhawna Suri, Ms. Shweta Taneja, , Nitesh Sahni Department of Computer Science, Bhagwan Parshuram Institute of Technology, Delhi, India.

[vi] Chung,& Iorga, & Voas, & Lee, (2017). "Alexa, Can I Trust You?". Computer. 50. 100-104

[vii] Burkett, C. (2018). call alexa to the stand: The privacy implications of anthropomorphizing virtual assistants accompanying smart-home technology. *Vanderbilt Journal of Entertainment & Technology Law, 20(4),* 1181-1218.

[viii] Y. Huang and G. Li, "A Semantic Analysis for Internet of Things," *2010 International Conference on Intelligent Computation Technology and Automation*, Changsha, 2010, pp. 336-339.

[ix] Ibarra-Esquer, J. E., González-Navarro, F. F., Flores-Rios, B. L., Burtseva, L., & Astorga-Vargas, M. A. (2017). Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. *Sensors (Basel, Switzerland)*, *17*6

[x] Norberg, F.E., & Yildirim, Z. (2018). The implementation of Voice Command in Smart Homes.

[xi] Marr, B., 2020. *Machine Learning In Practice: How Does Amazon's Alexa Really Work?*. [online] Forbes. Available at: <https://www.forbes.com/sites/bernardmarr/2018/10/05/how-does-amazons-alexa-really-work/#2949c301937f> [Accessed 9 March 2020].

[xii] Marr, B., 2020. *Machine Learning In Practice: How Does Amazon's Alexa Really Work?*. [online] Forbes. Available at: <https://www.forbes.com/sites/bernardmarr/2018/10/05/how-does-amazons-alexa-really-work/#2949c301937f> [Accessed 9 March 2020].

[xiii] Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; and Aharon, D. (2015)"*The Internet of Things: Mapping the Value Beyond the Hype."* McKinsey Global Institute

[xiv] GOV.UK. 2016. *Britain'S Cyber Security Bolstered By World-Class Strategy*. [online] Available at: <https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy> [Accessed 6 March 2020].

[xv] The Guardian (2013) NSA stores metadata of millions of web users for up to a year, secret files show Available at: http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents > [Accessed 9 March 2020].

[xvi] Harrison, L., 2020. *Fridges To Be Hit By Net Viruses*. [online] Theregister.co.uk. Available at: <https://www.theregister.co.uk/2000/06/21/fridges_to_be_hit_by/> [Accessed 7 March 2020].

[xvii] Neagle, C., 2015. *Smart Refrigerator Hack Exposes Gmail Account Credentials*. [online] Network World. Available at: <https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html> [Accessed 6 March 2020].

[xviii] Heartfield, Loukas, Budimir, Bezemskij, Fontaine, Filippoupolitis, Roesch, (2018)*A taxonomy of cyber-physical threats and impact in the smart home,*Computers & Security, Volume 78,

[xix] TechRadar. 2017. *What Is Smart Lighting? Everything You Need To Know For Your Connected Home*. [online] Available at: <https://www.techradar.com/uk/news/what-is-smart-lighting-everything-you-need-to-know-for-your-connected-home> [Accessed 11 March 2020].

[xx] Ring UK. 2020. *Video Doorbell 3*. [online] Available at: <https://en-uk.ring.com/products/video-doorbell-3?variant=32070268649565> [Accessed 4 March 2020].

[xxi] Samsung uk. 2020. *What Is Smart Lock And How Do I Use It? | Samsung Support UK*. [online] Available at: <https://www.samsung.com/uk/support/mobile-devices/what-is-smart-lock-and-how-do-i-use-it/> [Accessed 11 March 2020].

[xxii] Hern, A., 2017. *Fitness Tracking App Strava Gives Away Location Of Secret US Army Bases*. [online] the Guardian. Available at: <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases> [Accessed 7 March 2020].

[xxiii] Baker, C., Hutton, G. and Dawson, J., 2020. *Cyber Security In A Digital Age*. [online] House of Commons Library. Available at: <https://commonslibrary.parliament.uk/home-affairs/security/cyber-security-in-a-digital-age/> [Accessed 9 March 2020]

[xxiv] GOV.UK. 2020. *Secure By Design*. [online] Available at: <https://www.gov.uk/government/collections/secure-by-design> [Accessed 9 March 2020].

[xxv] Ronen, E., Shamir, A., Weingarten, A. and O'Flynn, C., 2018. IoT Goes Nuclear: Creating a Zigbee Chain Reaction. *IEEE Security & Privacy*, 16(1), pp.54-62.

[xxvi] GOV.UK. 2020. *Government To Strengthen Security Of Internet-Connected Products*. [online] Available at: <https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products> [Accessed 6 March 2020].

[xxvii] The Conversation. 2020. *The Dark Side Of Alexa, Siri And Other Personal Digital Assistants*. [online] Available at: <https://theconversation.com/the-dark-side-of-alexa-siri-and-other-personal-digital-assistants-126277> [Accessed 5 March 2020].

[xxviii] Heartfield, Loukas, Budimir, Bezemskij, Fontaine, Filippoupolitis, Roesch, (2018)*A taxonomy of cyber-physical threats and impact in the smart home,*Computers & Security, Volume 78,

[xxix]A. Oulasvirta, A. Pihlajamaa, J. Perki, D. Ray, T. Vh kangas, T. Hasu, N. Vainio and P. Myllymki (2012*), Long-term effects of ubiquitous surveillance in the home*, Proceedings of the 2012 ACM conference on ubiquitous computing, ACM pp. 40-50

[xxx] Pentestpartners.com. 2020. *The Most Common Iot Device Security Failings Of 2017 | Pen Test Partners*. [online] Available at: <https://www.pentestpartners.com/security-blog/the-most-common-iot-device-security-failings-of-2017/> [Accessed 9 March 2020].

[xxxixxxi] prpl Foundation (2016). Security Guidance for Critical Areas of Embedded Computing

[xxxii] Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). Alexa, Can I Trust You?. *Computer*, *50*(9), 100–104. https://doi.org/10.1109/MC.2017.3571053

[xxxiii] GOV.UK. 2020. *Secure By Design*. [online] Available at: <https://www.gov.uk/government/collections/secure-by-design> [Accessed 9 March 2020].

[xxxivxxxiv] Bullguard.com. 2020. *Despite Fast Adoption Of Internet Of Things, A Shocking 72 Per Cent Of Consumers Don'T Know How To Secure Their Connected Devices*. [online] Available at: <https://www.bullguard.com/press/latest-press-releases/2016/03-17.aspx> [Accessed 8 March 2020].

[xxxv] Wolfson, R., 2018. *Blockchain-Based AI Voice Assistant Brings Data Privacy To Smart Homes*. [online] Forbes. Available at: <https://www.forbes.com/sites/rachelwolfson/2018/09/14/blockchain-based-ai-voice-assistant-brings-data-privacy-to-smart-homes/#48ba4b946b50> [Accessed 11 March 2020].

[xxxvi] Blockgeeks. 2017. *What Is Blockchain Technology? A Step-By-Step Guide For Beginners*. [online] Available at: <https://blockgeeks.com/guides/what-is-blockchain-technology/> [Accessed 9 March 2020]