She Knows Too Much–Voice Command Devices and Privacy

Conference Paper · January 2019

DOI: 10.1109/ISSC.2018.8585380

2 authors:

Eoghan Furey
Letterkenny Institute of Technology
33 PUBLICATIONS 301 CITATIONS

SEE PROFILE

Juanita Blue
Ulster University
20 PUBLICATIONS 37 CITATIONS

SEE PROFILE

She Knows Too Much – Voice Command Devices and Privacy

Eoghan Furey [1], Juanita Blue [2]

[1] Department of Computing, Letterkenny Institute of Technology, Letterkenny, County Donegal, Ireland
[2] Intelligent Systems Research Centre, University of Ulster, Derry, Northern Ireland, UK

***Abstract*— Voice controlled Internet of Things (IoT) devices have become ubiquitous in homes and offer individuals many convenient and entertaining features. The Amazon Echo and its intelligent personal assistant, "Alexa", is a leading innovation in this area. This novel research examines aspects of privacy relating to personal use of the Echo. It aims to ascertain the types of data that may be vocally extracted from a selection of the multitude of applications that may be linked to the Echo.**

In the era of IoT, Big Data and Artificial Intelligence, privacy concerns are paramount for the individual. Personal data has never been more valuable, both to large reputable corporations and to criminals groups. The European Union's General Data Protection Regulations (GDPR) will come into force in May 2018, aiming to protect the personal data of EU citizens. This has further highlighted the emergent risks stemming from this technological medium.

This paper demonstrates that a typically configured Echo device can prove to be a vulnerable channel by which personal information may be accessed. Where no safeguards are implemented, a plethora of data including personal identifiable information and personal health information is available from the device. Data exposure by simple vocal request leaves the system vulnerable to inquisition by any unauthorized individual who is within "ear shot" of the device. The research explores the extent to which these risks can be reduced or mitigated, offering a set of recommendations aimed at preserving user privacy, while still enabling functionality of the device. Adherence to these recommendations will empower individuals to guard against privacy breaches from local sources.

Keywords— Personal Data; Privacy; GDPR; Voice Command Devices; Amazon Echo;

I. INTRODUCTION

Spurred by significant advancements in technology, increased availability and great reductions in cost, there has been an explosion in the popularity of voice-controlled Internet of Things (IoT) devices [1]. 'Voice Command Devices' (VCDs) allow users to access intelligent personal assistant services that are designed to synthesize various aspects of daily life [2]. Leading technological organisations market these devices as agents of convenience, providing a nucleus that manages the data relied upon to function in a complex world where individuals lead a detailed existence. Inviting these devices into one's home environment has many benefits, making life easier, expediting access to information and streamlining often hectic routines. However, along with the novelty and increased convenience comes a plethora of privacy concerns [3][4][5][6] that most users have not considered. The personal and home IoT revolution has the capacity to contribute a multitude of worthwhile and novel features that aid and improve the user experience when executing conventional tasks. IoT facilitates granular control of domiciliary routines, including adjustment of light, heat and other environmental amenities, managing entertainment such as music playlists, organizing meetings through calendars, making purchases, and even communicating with contacts. While a large proportion of individuals are happy to subscribe in order to enjoy the benefits provided by such tools, they neglect to acknowledge the implications of allowing intelligent technology to infiltrate their private lives [5][6]. The volume of personal information acquired and stored by such devices and supportive platforms is growing at an exponential rate [7].

When users purchase, configure and utilize these devices they are subscribing to a much larger and extremely profitable phenomenon. Intelligent devices, particularly smart phones and IoT hubs conduct data acquisition, transmitting the information back to the parent companies for analysis. The minutiae of individuals' daily lives are added to an extensive pool of valuable information that provides great habitual and economic insight and can be traded for a myriad of purposes. Information technology (IT) leaders such as Amazon, Google, Microsoft and Apple have invoked methods to utilize and exploit their access to this personal data, conducting analysis via machine learning algorithms [8]. Even more valuable than the profit from the sale of these devices, is the profit from the information that is harvested and sold to other various entities.

Personal data is not only valuable to large IT companies, it is also of great worth to groups and individuals who wish to use it for nefarious purposes such as social engineering, identity spoofing and identity theft [9]. Personal and home IoT devices manage many private details that link directly to individuals, and thus, have the potential to act as a central data cache for those with malicious intent.

In the era of the European Union's General Data Protection Regulation (GDPR) and heightened concerns relating to the protection of personal data and the preservation of privacy [8]; numerous questions have been raised by this new wave of technology. This research identifies a number of these uncertainties and through testing it explores the implications of linking devices and applications by a process referred to as 'daisy chaining' [10]. Personal data access and exposure, that may potentially result in foot-printing, social enumeration and identity theft is assessed. Finally, a list of guidelines will be outlined; these will provide advice on how individuals may better protect themselves and preserve the privacy of their personal data.

978-1-5386-6046-1/18/$31.00 ©2018 IEEE

II. Background

This section provides background for the research, offering information that relates to the technologies and privacy considerations concerned.

A. *Internet of Things (IoT)*

In recent years the volume of commercially available home and personal IoT devices has mushroomed. The trend grew from a select number of niche products manufactured by companies like Oregon Devices and Philips, to a large number of gadgets produced by IT manufacturers large and small. These devices bear the capacity to gather metrics and provide support for many aspects our lives [2]. The popularity and use of personal health monitors and connected home devices such as smart TVs, speaker systems, kitchen appliances, home heating and lighting options has become widespread and almost commonplace [11]. All of the major electronics and computing companies are now competing for this market, seeking to become leaders in the IoT race.

The majority of these IoT devices depend on some form of central hub that facilitates an internet connection and links to the parent organisation's cloud. Personal computers, tablet devices and particularly smart phones execute this functionality by hosting a controlling software application (app) and acting as the gateway to the internet. While keyboard and pointer input have traditionally been the means of human-computer interaction, there has been a significant drive since 2012 [12] to enable hands free control, primarily by voice control. Applications such as *Google Assistant* have exposed and familiarized users with voice control and encouraged them to adapt to more convenient methods of technological input and interaction. Figure I depicts the operation of Voice Command Devices.

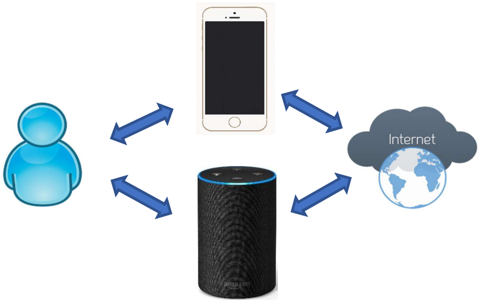

Figure I: VCDs connect to the Internet & Cloud

B. *Voice Command Devices & Voice User Interface*

Apple's Siri, Microsoft's Cortana and Google Assistant have improved and enhanced the technology supporting vocal interaction with VCDs though Smart phone applications [2][12]. The Amazon Echo and Google Home have significantly improved the functionality and usability of VCDs, providing access to intelligent features via Smart Speakers. Based on research conducted, as of 2018 the Amazon Echo is the market leader [13], sporting the largest selection of compatible devices and applications.

<u>*Amazon Echo*</u>

The Amazon Echo provides an intelligent personal assistant referred to as 'Alexa', who possesses a range of functionality which enables voice activation and communication with numerous IoT devices and applications, examples of which are outlined in Table I. To interact with Alexa, a user simply has to speak the 'wake' word "Alexa" or one of three other wake word options offered by Amazon. Alexa is configured by default to respond to any user's voice, however the device does possess a voice recognition feature that can be activated through the settings. This feature will train the VCD to implement biometric authentication and only respond to a single user's queries.

Table 1: Examples of information available from Echo's Alexa

Information Type	Questions asked
Sleep Patterns	
	• **Waking and bedtime routines** • **Lights, heating and coffee making** • **Fitbit sleep patterns**
Contacts	
	• **Who is on your contacts list for Alexa calling** • **Who you are meeting with via schedulers**
Interests	
	• **Music tastes (Amazon music, Spotify)** • **Reading and audio books (Audible)** • **News and Hobbies (Personal news feeds and sports)** • **Search history**
Personal Health Information	
	• **Exercise and Fitness levels** • **Resting Heart Rate, Steps per day (Fitbit)** • **Sleep patters**
Location and Travel	
	• **Commute to work, Traffic** • **Meeting schedules and locations** • **Find my phone**
Dietary requirements	
	• **Shopping lists** • **Restaurant reservations**

Various IoT devices can be configured to link to the Echo, subsequently allowing users to interact with those devices via voice control. Whilst interactive activities vary depending on the purpose of the functionality of the IoT device, most devices will allow access to their status and elements of their associated data. Users may verbally query linked devices and the results of these queries will be reported vocally via the Echo speaker system [6][11][12].

The process of linking devices and application accounts via a central hub is referred to as 'daisy-chaining' [10]. When daisy-chaining is implemented, the Echo becomes almost omniscient, acting as a central source for information associated with the devices, their platforms and also personal details related to the individual. Depending on the purpose of the device, these may include personal health information, habits, location and much more. The Echo harvests all the data it is exposed to and transmits it back to Amazon's cloud. Deep Learning algorithms are then applied to customise the user experience and improve the service [14].

C. *IFTTT*

IF This, Then That (IFTTT) is a free framework that allows users to daisy-chain their devices and associated accounts [15]. The framework enables communication between devices and applications which may not have been specifically designed to connect and transmit data between each other. The idea for IFTTT grew out of the belief that, in the future, everything will be a service, virtually every appliance and gadget we use will be connected to the internet or tracked by the internet of things [16].

Using IFTTT in conjunction with Amazon's Alexa voice assistant is becoming increasingly popular for users who wish to create 'rich interactions' with their smart devices, services and apps. Examples of these links may include asking Alexa to make a cup of coffee with WeMo's connected coffee maker or changing the color of Hue smart lights each time Alexa plays a new song. However, exposing personal data to an untrusted third party app introduces countless privacy vulnerabilities [16].

D. Data Protection

The EU data Protection Directive (95/46/EC) defines personal data as " *'personal data' shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*" [17]. This broad definition is designed to cover any personal data that directly relates to an identifiable living individual.

Data protection refers to an individual's fundamental right to privacy. Where personal data is collected, stored and processed, there are a number of stakeholders who are legally responsible for protecting that data and ensuring the preservation of privacy [18]. Entities that control the collection and use of personal data are referred to as 'Data Controllers'. These may be individuals such as medical practitioners, financial institutions, organisations such as Facebook and Amazon, or government departments such as Social Welfare. Data Processors are entities who process personal data on behalf of a data controller, but do not work directly for the data controller [18]. An example of this might be a payroll company or an analytics company working for a large retail store.

E. General Data Protection Regulations (GDPR)

In 2016 the European Union (EU) introduced the General Data Protection Regulations (GDPR). These regulations will come into force on the 25th May 2018 and are the biggest change to Irish data protection legislation in twenty years. Technological advancements have necessitated uniform EU implementation of new regulation that acknowledges the advent of emerging technology and services including the Cloud, the IoT and AI. This has heightened concerns over the legal and ethical collection and use of personal data [18].

The new GDPR is a regulation and compliance issue that places greater legal obligations and accountability on data processors. Data processors must comply with the new regulations or face large fines. These changes effect organisations such as cloud providers and analytics firms who are processing data that relates any EU citizen, regardless of whether they operate within the EU or in another jurisdiction [16].

Interestingly, only eight of the ninety-nine articles in the GDPR deal specifically with technology and tools, however all manufacturers of IoT devices who serve European consumers will be subject to the new regulation [17]. IoT device Terms and Conditions must clearly state what any data stored in the cloud will be used for and must notify customers of any changes in processing [19].

One of the ripple effects of the GDPR is that it has aroused a global recognition of the significance of personal data [18]; including an individual's fundamental right to the protection of the privacy of their data. However, Personal Health Information gained from wearable IoT devices is not directly addressed by the GDPR, despite its sensitive nature.

F. Privacy Challenges with the IoT

In 2018 it is estimated that 80% of the world's data has been created within the last two years [20]. The use of IoT devices has further increased the quantities of data that are being gathered, stored and analysed. Applying Artificial Intelligence (AI) to this data has increased its value and enabled direct monetization via targeted and bespoke advertising and recommendations [11][12].

From a consumer perspective, there is a distinct lack of transparency and accountability relating to the large amounts of data that are generated. Organisations fail to explicitly state the purposes for which they process this data and the methods they invoke to do so. Furthermore, the sources and recipients of the data remain largely unknown by the very individuals who are generating the data.

Personal data collected and processed in this manner may appear innocuous, but in the era of privacy breaches [21], when inferential data is combined it can form a rich profile of an individual [22]. Despite a multitude of available compliance standards such as ISO 27018, which are intended to protect systems from security breaches; these documents do not directly address the privacy issues pertaining to personal data that is housed in 'secure' and 'compliant' systems [23].

Privacy refers to legislation and regulations governing the legal collection, processing, sharing, transfer and storage of data [24]. Although cyber security and preservation of privacy are linked, they are two distinct areas which require specific forms of attention to ensure confidentiality risks are mitigated.

Personal Identifiable Information (PII) and Personal Health Information (PHI) are two types of information [25] collected and processed by the Echo and similar VCD devices. Through daisy-chaining, consumers may link wearable health trackers to their intelligent personal assistants as a convenient method of querying their own metrics and attributes. Although the IoT device manufacturers may acknowledge and outline collection and processing within their own Terms and Conditions, the incorporation of a VCD creates a unique vulnerability [1][5][6][11][23].

When devices are configured and synced, any individual within range of the VCD may issue verbal queries relating to this data. PII can be extracted easily from connected devices such as wearable health monitors [26]. This relates to data which may divulge social interactions, location history, purchase history and hobbies or interests of an individual. PHI may divulge information such as location history, step count, heart rate and also the times and duration of sleep [26]. This unverified access poses a serious threat to the privacy of data that is generated by IoT devices [27].

Although dubbed 'intelligent' based on their learning capability, automated personal assistants such as Alexa lack the very important human ability to discern which information should be shared and who can be trusted. Traditionally information systems have relied upon identity authentication and defined access levels to determine whether data can and should be shared. Experiential learning enables humans to do the same and be cautious about protecting privacy and personal information. Intelligent personal assistants currently do not possess the nous that enables them to make these decisions in a trustworthy manner.

III. Methodology

The aim of the experiment was to determine what personal information could be gained from a VCD through voice queries. Researchers wished to establish if the security of the authorized user's identity could potentially be compromised by an unauthorized actor's inquiries. Although some of the information sought may also be gained through traditional social engineering methods, the VCD had the potential to behave as a central source for the data, simplifying and expediting the process of foot-printing and social enumeration.

A script was developed that outlined queries to be posed to the Echo VCD. These questions were designed to test data accessibility and identify the types of personal information that could be gained, without any requirement for the inquirer to authenticate either verbally or through the smart phone. Each of the questions sought information that potentially contained PII or PHI or may be considered 'personal' in relation to privacy and GDPR concerns. This testing was intended to determine how much personal information could be elicited from Alexa. An excerpt from the tested script is depicted in Section IV.

A test environment was constructed where an Amazon Echo VCD with default configuration was linked to several accounts, applications and IoT devices through the standard settings. It should be noted that an Amazon account is a mandatory requirement for configuring the Amazon Echo. For this experiment the devices were all configured with the username "John". Table II lists the devices, accounts and applications that were daisy-chained for testing purposes.

Following configuration of the test environment, an 'unauthorized actor' was granted a 5 minute time limit to interact with the VCD while the linked smart phone was not within range of the device. The actor was familiar with Alexa functionality, the wake word "Alexa" and the username "John". The actor posed each of the questions contained within the script to the VCD and created an audio recording of the responses. The same script was then tested after activating the voice recognition feature of the VCD. This second test was conducted in a bid to ascertain if this mechanism was successful in preserving user privacy. See Section IV.

Table II: Devices, Accounts & Applications Linked for Testing

Test Environment
Devices
• **Amazon Echo 2nd Generation VCD**
• **Fitbit Surge Wearable Health Tracker**
• **Samsung Galaxy S5 Smart Phone**
• **Standard Wireless Modem with Broadband Connection**
User Accounts
• **Amazon Account (online shopping)**
• **Amazon Music Account (streaming music)**
• **Audible Account (audio books)**
• **Fitbit Account**
Applications
• **Fitbit**
• **Microsoft Office 365 (calendar/email)**
• **Alexa Traffic (home & work locations)**
• **Alexa Routines (start my day: weather/news headlines)**
• **Alexa Shopping List and Reminders**
• **Smart Home (appliances & amenities)**
• **Alexa Your Voice (authorized voice access/recognition)**
• **Alexa Calling & Messaging (Alexa enabled devices)**

IV. Results

This section offers an excerpt from the query script and responses in Table III. In addition, included is a summary of the information gained with and without the voice recognition feature activated. A brief analysis of the results is discussed, identifying the potential vulnerabilities and risks associated with unauthorized person(s) accessing information through a daisy-chained VCD.

Table III: Script of Questions

Excerpt from Query Script	
Q1	**Alexa, ask FitBit what my Resting Heart rate is.** *Your resting Heart rate is 53 beats per minute*
Q2	**Alexa, ask FitBit how did I sleep** You fell asleep at 11.30 pm and slept for 6hrs 45mins
Q3	**Alexa, what is on my shopping list?** *Bottle of coke, Pasta, 3 bottles of white wine*
Q4	**Alexa, where do I live?** *Your home location is [town name, longitude and latitude]*
Q5	**Alexa, what's on my calendar?** *Here are the next four events, at 9.30 am meeting with MSc student, 10.30 am meeting with Thomas, 11.30 Computer architecture class, 4pm Meeting with Open Cloud company*
Q6	**Alexa, play my messages** *One from Michael: Please call me regarding the meeting*

The results in Table IV demonstrate that in use-cases where Alexa has access to the information associated with linked accounts, she will divulge that information without any requirement for authentication by the user. Access to data contained within linked devices and applications is readily available to any inquirer within voice range of the VCD, regardless of whether or not they are authorized or the linked smart phone is within the same range.

The tests conducted indicate that VCDs lacking any implemented security mechanisms will share personal information with unauthorized individuals. This poses serious security risks to the personal data pertaining to the linked applications and devices. Such vulnerabilities have the potential to facilitate crimes ranging from burglary to fraud and also identity crimes such as identity spoofing and identity theft.

The large majority of technological devices in the modern day require some form of authentication to access data, these may include something you know (password or pin), something you have (card or token) or something you are (fingerprint or other biometric). Based on this premise, the unprotected VCD used in testing is non-compliant with standard minimum security recommendations which state that authentication must be required to ensure that only authorized persons may access data.

It should be noted that the Alexa application does include a voice recognition feature included which allows the VCD to learn and recognize the primary user's voice. As demonstrated by the results in Table IV, enabling this biometric feature limits unauthorized access to information, acting as a control to mitigate the risk of unauthorized persons querying the VCD. However, it must be stated that when configuring the device for use, there is no manufacturer advice suggesting this feature should be activated in the interests of security and privacy.

This is further exacerbated by the fact that users may believe that their linked smart phone device (which may have a security pin implemented) must be in range to utilize the VCD and acts as a security mechanism (token). As demonstrated by the tests conducted, this is not the case. An unsecured VCD can and will act as a central point of accessible personal data, without verification of identity.

Table IV: Results of Alexa Queries

Information sought	Function queried	Information returned?	
		Without Control	With Control
Current location	Find phone	Yes	No
Work location	Commute	Yes	No
Music preferences	Amazon music	Yes	No
Current Heartrate	FitBit	Yes	No
Resting Heartrate	FitBit	Yes	No
Steps count	FitBit	Yes	No
Sleep quality	FitBit	Yes	No
Food preferences	Shopping list	Yes	No
Drink preferences	Shopping list	Yes	No
Volume of drink	Shopping list	Yes	No
Home location	Commute	Yes	No
Sleep location	Commute, FitBit	Yes	No
Hobbies	Search, routines	No	No
Contacts	Drop-in, Alexa calling & messaging	Yes	No
Schedule	Outlook calendar	Yes	No

Table IV summarizes the results, detailing the personal information that was sought about the primary user. The table outlines which function was used to access the data and those queries that successfully extracted the information from the device. The table also indicates whether the same information could be successfully extracted when the voice recognition biometric control was activated. The results indicate that activation of the voice recognition biometric control was successful in preventing an unauthorized person from accessing the data linked to the VCD.

V. Recomendations

As demonstrated by testing and results, use of VCDs configured to link to other IoT devices, accounts and applications pose a serious threat to primary user privacy and identity. This section outlines a list of recommendations that may be implemented to reduce the risks associated with this type of IoT device.

i. Do not daisy-chain devices unless necessary.

ii. Set up individual voice recognition for the primary user (biometric authentication).

iii. Consider whether convenience is more valuable than privacy when linking accounts to the VCD. Possibly create a new account, if access to contacts and calendar are not required. Ensure this account is authenticated with a strong password.

iv. Change the default 'Wake Word'

v. Beware of third party applications such as IFTTT, as these applications may significantly increase the attack surface by introducing new vulnerabilities.

vi. Set a password or turn off the purchasing mechanism if it is not required.

vii. Ensure the main account linked to the device invokes a minimum of two-factor authentication including strong password.

viii. Configure the Wi-Fi network with WPA2 encryption and do not use an open hotspot.

ix. Turn off the VCD at the power when not in use.

x. Overall, consider carefully the potential implications of linking any device or account to a VCD. Do not link any accounts containing information that is intended or required to remain private.

VI. Conclusion

Voice Command Devices are becoming ubiquitous within our homes and will soon be appearing on our workplace desks too. These devices offer support and convenience, fulfilling the role of a personal assistant, but unlike a human assistant they lack the nous to identify what information should be considered personal and thus kept private.

While the Echo sports a finite number of security features which may be configured by the user, the effectiveness of these mechanisms remains limited. This is particularly apparent with the device wake words, where the manufacturer only allows four previously defined options. Theoretically the wake word could operate as a password in future device versions. Preservation of privacy is reliant on the users implementing measures in order to protect their own data. In addition, currently VCD manufacturers fail to recommend that activation of these features is an important element of safe and secure use of the devices. Where this information is lacking, many individuals may not have the security expertise or indeed even care about what data the VCD controls. Thus, their personal data remains compromised.

This study strives to raise awareness by demonstrating the variety of personal information ranging from PHI to PII which may be easily elicited from the Amazon Echo. In light of the upcoming GDPR and a plethora of recent data breaches, the privacy and vulnerability of personal data is more topical than ever. Compliance with GDPR remains the responsibility of the parent company, however these regulations are only relevant within the defined responsibilities of the Data Controller and Data Processor. When a user agrees to the terms and conditions, they agree to both the processing of their data and to allow it to be accessed by the VCD. Ultimately, when linking IoT devices, the security of personal data is the user's responsibility and many users will fail to configure security features available, resulting in significant risks to their own privacy and also enhancing the risk of further crimes.

The commonly feared 'security of data in the cloud' may not be VCD technology's true weakness, GDPR has this covered. The real vulnerability lies in the user's own portal to conveniently access their data. If this is unsecured, privacy risks are increased significantly. VCDs have cultivated an environment where one who seeks information, only has but to ask!

As of 2018, the sales and ubiquity of these devices and the information they contain looks set to grow at an ever increasing rate. In the future these devices may become more sophisticated and discerning about what information they share and with who; however, for the moment a simple question asked within a earshot will have them singing like a bird!

REFERENCES

[1] Trusted Devices in the Context of IoT," 2017 Euromicro Conf on Digital System Design, Vienna, pp. 502-509, 2017.

[2] López G., Quesada L., Guerrero L.A. "Alexa vs. Siri vs. Cortana vs. Google Assistant: A Comparison of Speech-Based Natural User Interfaces". In: Nunes I. (eds) Advances in Human Factors and Systems Interaction. AHFE 2017. Advances in Intelligent Systems and Computing, vol 592. Springer, Cham, 2018.

[3] Baldini, G. et al., "Ethical Design in the Internet of Things". Science and Engineering, Ethics, pp.1–21. 2016

[4] Sauer, G., A Murder Case Tests Alexa's Devotion to Your Privacy | WIRED. https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/, February 2017.

[5] Symantec Corporation., "A guide to the security of voice activated smartspeakers", https://www.symantec.com/content/dam/symantec /docs/security-center/white-papers/istr-security-voice-activated-smart-speakers-en.pdf, 2017.

[6] Boughman, E., "Is There An Echo In Here? What You Need To Consider About Privacy Protection". Forbes Legal Council. https://www.forbes.com/sites/forbeslegalcouncil/2017/09/18/is-there-an-echo-in-here-what-you-need-to-consider-about-privacy-protection/#395461bb38fd, September 2017.

[7] Conti, M., Dehghantanha, A., Franke, F., Watson, S., "Internet of Things security and forensics: Challenges and opportunities", Future Generation Computer Systems,Volume 78,Part 2, Pages544-546, 2018

[8] Storr, C., Storr, P. "Internet of Things: Right to Data from a European Perspective". In: Corrales M., Fenwick M., Forgó N. (eds) New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation. Springer, Singapore, 2018.

[9] Van Till, S., "The Five Technological Forces Disrupting Security: How Cloud, Social, Mobile, Big Data and IoT are Transforming Physical Security in the Digital Age". Butterworth-Heinemann, 2017

[10] Pyeon, H.B., Kim, J.K. and Oh, H., Conversant Intellectual Property Management Inc, "Daisy chain cascading devices". U.S. Patent 9,240,227, 2016.

[11] Biljana, L., Risteska, S., Trivodaliev, KV., "A review of Internet of Things for smart home: Challenges and solutions", Journal of Cleaner Production,Volume 140, Part 3,Pages 1454-1464, 2017.

[12] Goksel Canbek, N., Mutlu, M., "On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants", Journal of Human Sciences, vol 13, no1, 2016

[13] Kinsella, B., "Amazon Alexa Smart Speaker Market Share Dips Below 70% In U.S., Google Rises to 25%", https://www.voicebot.ai/2018/01/10/amazon-alexa-smart-speaker-market-share-dips-70-u-s-google-rises-25/, February 2018.

[14] Anders, G., "Alexa, understand me" https://www.technologyreview.com/s/608571/alexa-understand-me/, August, 2017.

[15] Ur, B., Pak Yong Ho, M., Brawner, S., Lee, J., Mennicken, S., Picard, N., Schulze, D. and Littman, M.L.,. "Trigger-action programming in the wild: An analysis of 200,000 IFTTT recipes". In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 3227-3231). ACM, 2016.

[16] Surbatovich, M., Aljuraidan, J., Bauer, L., Das, A. and Jia, L., "Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes". In Proceedings of the 26th International Conference on World Wide Web (pp.1501-1510), 2017

[17] Regulation, E.U., "679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". Off J Eur Union, p.L119, 2016

[18] de Hert, P., Papakonstantinou, V., "The new General Data Protection Regulation: Still a sound system for the protection of individuals?". Comp. Law & Sec. Review, 32(2), pp.179-194. 2017

[19] Regulation, E.U., "679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". Off J Eur Union, p.L119, 2016

[20] Vishal, K., "Big Data facts", https://analyticsweek.com/content/big-data-facts/, August 2017.

[21] Blue, J., Furey, E., Condell, J., "A novel approach for secure identity authentication in legacy database systems", 28th Irish Signals and Systems Conference (ISSC), 2017

[22] Kostkova, P., Brewer, H., de Lusignan, S., Fottrell, E., Goldacre, B., Hart, G., Koczan, P., Knight, P., Marsolier, C., McKendry, R.A. and Ross, E., "Who owns the data? Open data for healthcare". Frontiers in public health, 4, p.7, 2016.

[23] Spiekermann, S., Acquisti, A., Böhme, R. and Hui, K.L., "The challenges of personal data markets and privacy". Electronic Markets, 25(2), pp.161-167, 2015.

[24] Singh, J., Powles, J., Pasquier, T. and Bacon, J., "Data flow management and compliance in cloud computing". IEEE Cloud Computing, 2(4), pp.24-32, 2015

[25] Daubert, J., Wiesmaier, A. and Kikiras, P., "A view on privacy & trust in IoT". In Communication Workshop (ICCW), 2015 IEEE International Conference on (pp. 2665-2670). IEEE, 2015

[26] Graziano, D., "Amazon's Alexa can now update you on your Fitbit progress", https://www.cnet.com/news/amazons-alexa-fitbit-integration/, March 2016.

[27] Wheatley, S., Maillart, T., Sornette, D., "The extreme risk of personal data breaches and the erosion of privacy". The European Physical Journal B, 89(1), p.7, 2016.