Ethical Review on Home Assistant Devices

Prepared by

Yiwei Liu (1145366)
Mounik Patel (1144127)
Jay Patel (1134858)
Samip Karbhari (1146116)

Under the supervision of

Prof. Abhijit Rao

Submitted at

Lakehead University

DEPARTMENT OF COMPUTER SCIENCE

Table of Contents

Executive Summary

We discussed home assistance devices, how it came into focus and how it works, issues related to smart devices, facts and key stakeholders discussed. Then we applied 3 different frameworks to explore ethical perspectives. First was the humane design framework, in which we saw how these devices affect human emotions, decision making and sense making capabilities. Second was the good, clean, fair framework; in which we talked about whether these assistance systems are socially acceptable or not, are these products environment friendly or not, and is this fair for all the stakeholders like workers who make these systems, designers. In the IEEE framework, other perspectives like privacy and risk of algorithm and sensor failures were discussed. On the other side, we also described some benefits of using home assistance devices. After discussing issues, we provided some existing solutions which are very helpful to control these technology drivers and proposed some solutions also. Solutions were proposed for how users can help us to make products that are more reliable, could we manage our data, and how to tackle e-waste.

1. Introduction

Nowadays, there are thousands of Home assistant services out there in the IT and business market for everyone to choose from. Decades ago, people would not believe that they can control their home lighting and air conditioning or having their own coffee machine to make coffees simply by tapping the smartphone or making a voice command without physically being at home or performing any actions.

This innovative blueprint started with Microsoft co-founder Bill Gates demonstrating his smart home "Xanadu2.0". In Bill Gates's home, the guest will be wearing an electronic pin, the smart home sensors will locate the guest position and provide preferred lighting, room temperature and humidity, music and art display. Such manifestation incepts the home assistance idea into everyone's heart and brings the IT industry a new path to proceed. Years later, with the technical progress we made and the leap in productivity, home assistance is no longer a billionaire-only service. Home assistant services became more accessible and affordable in our daily life, in the meantime flexible enough to compact with other smart "Internet of Things (IoT)" devices though different commercial brands.

Currently, we have several internet giants making eye-catching products in the home assistance area such as Amazon Echo, Apple Home Pod, Google Nest and etc. Those products are normally designed as some type of speaker and paired with intelligent personal assistants like "Alexa", "Siri" or "Hey Google". Generally, we use it to set up timers and reminders, listen to news and music, or even do shopping. And since it is a speaker, it is hands-free and can be used by multiple family members. Because of those features, such products would collect our basic family information like members' names, gender, preference and life routine.

And some of those home assistant products have collaborated with other IoT brands to control and manage all the IoT household appliances in the home. For example, Amazon Echo and Google Nest can direct your iRobot vacuum cleaner to do the housework, Apple Home Pod and Google Nest can easily play your favorite show on your LG TV without actually using the controller. With all the IoT devices connected to the home assistant, those home assistants will have further information about the home layout, appliances' usage data or even access the cameras and microphones in the house.

Remote control, hands-free, voice command, home assistant products not only bring a lot of conveniences compared with the traditional analog devices but also add a tint of science fiction movie aura into our daily life. Unfortunately, more concerns about abuse of privacy and home security problems came to our attention. Our team would like to dig into the ethical issues around the home assistant devices and services, looking for the potential menaces and unfairness and try to provide mitigations.

2. Current Situation

a) Issues

Since home-assistant devices have gained popularity in today's world, it is necessary to understand the risks and issues faced during their usage. While most of these devices have already included some cybersecurity mechanisms in their design, there is still a significant number of security and privacy challenges that need to be addressed. We will be discussing such issues and challenges in this section.

According to Statista figures, there will be about 82.5 million home automation systems by the end of 2021. [1] While these devices have helped us connect and control numerous other devices in the home with the help of a smartphone, they have also become a family member without even our consent. They know what we like to eat, what we like to wear, what we like to do in our free time as our family members know about us. We might think that these devices are flag bearers of future technology, but they have breached privacy in recent years like no other technology. These devices embedded with multiple sensors, software and different technologies are vulnerable and can be easily hacked and used for eavesdropping on us by tracking and monitoring our daily activities. [2] These devices automatically collect, and exchange data related to us over the internet without our consent. [2]

The data which is collected and exchanged over the Internet without our consent is utilized by major technology companies who proliferate and expand its services to a big set of the population nowadays for free of cost. [2] These companies use 'Targeted Advertising' as their business model and generate revenues by sharing user's data to anonymous third-parties such as advertisers and marketers. [3] The third-party companies collect, exchange, and analyze the data using various analytical (Machine Learning) techniques to create advertisements and sell their products to targeted users. [2] The data which is analyzed is used to provide advertisements from third-party companies to lure the user into buying their services and products. This affects the sense-making process of users, who do not want to buy any of these services or products end up owning one.

As a human being and a social animal, we have a need for other people to know what we are doing, talking, and thinking about, which is the reason why we are so active on social media since it has started booming. But on the same note, we as a human being would like to have our rights of privacy and freedom accounted for so that we can do any sort of activity and be free of the people’s judgement. [4] There is all type of things that we do, we talk and think about which we want to share only with our family, friends, lawyer, physician, psychiatrist and do not want to share it with the rest of the world. This is the reason why privacy matters and it is very valuable to humans. [4] There are a lot of psychological studies that have been done on this basic human nature which proves that our behavior and actions become restricted while we are in a state of constant surveillance. [4] These home-assistant devices can be easily hacked and used to monitor our daily activity, breaching our right of privacy. It affects the user's psychological characteristics and emotional capabilities as they live in constant fear that they are under 24*7 surveillance. User's range of behavioral choices also drastically change when they know they are regularly monitored. [4] It also affects the decision-making process of users, who

might not be able to make decisions efficiently and effectively since they are worried by the privacy breach and constant monitoring by the home-assistant devices.

Patrignani et al describes a Good ICT in their paper as “socially desirable”, which means all the devices and technologies are developed keeping the human needs in mind and the technology must be human-centered. [5] The home assistant devices are developed in such a way that they are generally triggered or controlled using either our voice or using the smartphone. Most of them are controlled by voice-enabled commands where the devices verify the user’s voice and assist for the command given. By design, the user verification is done using ‘wake-up words’ that are recognized locally in the device. [6] User is given a set of options to select a wake-up word from a set of predefined options. It is very easy for a hacker to find the wake-up word of the user. [6] In addition to this, there is no further authentication of user is done from the home-assistant devices and they will accept any command following the wake-up keyword. [6] This type of design does no good to user, as they are sold to them with the belief that they will be the sole owner of these devices and they will be controlling them. But the truth is that it is easy for anyone in proximity to issue commands to these devices.

These home-assistant devices keep constantly listening to the users’ conversation while waiting for a wake-up word. If a user says wake-up word or any phonetically similar words accidentally, then the home assistant device will be triggered and it will start recording the whole conversation by users. [6] Consequently, this conversation can be uploaded to the Internet which directly affects security and privacy of the user. These private or confidential conversations can be accidently leaked, or any sensitive information can be hacked by someone. [6] This example shows that the users are not in total control of their voice data. The scenario mentioned here is very common during usage of home-assistant devices and hence, they pose serious concerns to one’s privacy.

A technology should imply equitable use for all, and it should be simple and flexible in use, as per the norm of the ‘Universal Design Principles’. [5] The home-assistant devices are developed for multi-user environment, by default keeping in mind that all the users in a household can use them equally. But the absence of granting proper accessibility rights to different levels of users lead to a serious vulnerability. Although, most of the home-assistant devices give an option of ‘primary user’ who has the accessibility for all controls of the devices, there are many other important controls and commands which can be given by the rest of the users of the household. [6] This leads to some serious design faults and issues where anyone can take over the control of the device and modify the settings accordingly.

IoT devices are made up of circuits and small mechanical parts, which may not work correctly due to overheating and many other factors affect it [7]. As we are using smart TVs, refrigerators, air conditioners and many more smart devices which contain a lot of sensors. We can operate all these devices through a single home assistance device, all these device sensors send data to home assistance devices. So, if any sensor sends wrong data, it may turn into some big serious issue. It may harm human life and play a role in making algorithms unstable. We consider examples of smart fire distinguish systems, if the sensor fails it cannot be able to recognize if there is fire or not. So, if sprinklers do not react at the correct time, it may harm a lot of human life.

Companies who make these home assistance devices use a lot of data to analyze patterns and then train algorithms which can react to any situation. But, what if as we

discussed above, as the sensor fails, the algorithm cannot know the real situation and may take wrong actions. Other than, no one can predict every situation in which this algorithm may have to work, if algorithms face new inputs from sensors which are different from training data may turn into risky behavior of the algorithm. If we consider example of self-driving cars, we need tons of data to train a self-driving car, but no one knows in uncertain situation like if car has to save a human and a dog at same time, it cannot find solution which can save both or it cannot make new type of prediction, which end up into loss of one life either human or dog [7].

As all the work done by home assistance devices is based on some commands or based on analysis of our daily routine, we don't need to remember everything now. So, if we use these kinds of devices from a very young age, it may affect our memory and we develop the habit of forgetting small things easily. If we consider an example, our parents and grandparents were able to calculate some basic math sums without using calculators and very fast, if we compare ourselves with them as we use calculators we don't even remember math tables. In school we mugged up those tables but now we forget as we didn't use our memory to calculate instead we use calculators. In the same way people are forgetting to turn off the lights, taking medicines on time and many more small things in daily life, which is the result of using this kind of technology.

Making physical property damage/loss. We can consider this case as a part of a privacy issue. We know that home assistance devices send data to servers and are always connected with the internet, so there are chances of hacking. And there are a lot of types of hacking. One can monitor your system and make changes without your permission. They can eject viruses that can use your personal device to access other devices and it may harm or destroy our system. For example, a WannaCry virus was ejected in one device and those corrupted devices were not in control of the owner, because of that virus so many companies have to bear big losses. To prevent our home assistance system from this kind of attack may cost us more as we have to hire 3rd party software for security.

There are a lot of companies who are making home assistance systems. And if we see the current trend in software, companies are providing premium plans, so if one wants to use their device up to full capacity, they need to purchase that premium plan for a month or a year. As we all are discussing ethics, technology should not be developed for individual purposes and should be the same for all, which is not preserved by any of these companies. And if one company does that then rest all will do the same, so choosing one is difficult as all the companies are making money from this kind of memberships and to collaborate with any other brand. For instance, we have Amazon Prime, Netflix membership, and a lot of online platforms are providing this kind of membership through which we can use their product without advertisements and up to its full extent.

b) Benefits

We described a lot of issues above, but there are several benefits which we cannot overlook. As we all know how difficult life handicapped people are living in. They can't easily do daily activities like us, where this kind of technology can help them to simplify their life and with one voice command they can do what they want. They can book uber, make coffee, order food, make payments and do a lot of daily work [7].

Other than that, we can think of a family who has a very busy schedule to work in. After coming from office, one wants to sit sometime and get some relaxation. These devices can turn on the air conditioners for us, they can also turn on the oven, so we get food ready when we reach home and like this there are many smart devices working together to provide comfort in our daily life. Another example is, we easily forget what things we need to prepare daily food, and now we have smart refrigerators that can inform us which products we need to purchase and can take note of products' health and quality also. There are a lot of things which we don't have to do on daily basis, for instance taking medicines, shopping and many more like this. So, home assistance devices are useful too.

3. Ethical Analysis

a) Key facts

Home assistant devices and services is a huge growing market. With nearly 80 million of smart home automation systems installed worldwide [1]. The research shows that this market is continuously growing globally and will reach more than 50 billion USD market size by the end of 2022 and would probably keep spiking to roughly 170 billion USD by the end of 2025 [9]. Right now, 45% of the smart home market revenue came from the US and 30% of the revenue came from China [10].

Currently, the most popular home assistant device is the voice assistants speaker and Amazon Echo is holding 62% of the market making Amazon leading in this competition [11]. Increasing numbers of the real estate buyers are proffering built-in smart HVACR (heating, ventilation, air conditioning and refrigeration) systems as well as smart locks and smart lighting. Home assistant related IoT market also grows rapidly. Over 20 billion IoT devices are used worldwide, and this market will continue extending its revenue over 520 billion by 2027 [12].

One of the benefits of having home assistant devices is time money, according to Consumer Reports, having a full set of smart home security systems would save up 20% of the house insurance premiums. And study shows that a house with home automation systems would reduce up to 15% of traditional energy usage [13], making the house more eco and saving more utility cost. This indicates why buyers are more inclined to real estate with prebuilt smart home systems.

On the other hand, more researchers are starting to focus on the potential privacy and security issue alone with the home assistant boom. Study shows that roughly about 40% of the smart home systems are operating one or more vulnerable IoT devices and devices with weak hardware security design could put the whole system endangered causing potential economic loss [14]. People were also concerned about personal privacy as a lot of personal data was collected and shared by the carriers and the collaborated IoT brands [15].

b) Key stakeholders

Major stakeholders for smart home assistant devices include: customers/buyers, sellers and brokers, and producing companies. Customers may include families installing technology in their houses, industrial companies, vacation rentals and hospitality service provides, health care facilities, etc. Users can further be divided into age groups such as young, middle, and old age.

It may happen that some of these stakeholders may not have complete understanding about the technology. Information and consent are important tools for protecting the autonomy, dignity and well-being of an individual. For instance, it is often difficult for older adults to make a decision about accepting or refusing smart home technologies, especially if they do not have sufficient information. [11] Many older adults are not familiar with the mechanism of information gathering and sharing through

technologies and may have a lack of technical understanding, they might not be well aware of the importance of protecting private information.

Thus, all stakeholders must acquire complete information regarding smart home assistant devices prior their installation. They should avoid having any misperceptions regarding the functionality of technology. Furthermore, multiple consents should be obtained from all the stakeholders who are involved in the technology.

4. Ethical considerations

a) Humane design guide

The basis for Humane design is to understand how the home-assistant devices affect the human sensitivities. Here, Human sensitivities are defined as human instincts that are often vulnerable to any new technologies. [16] The Humane Design Guide developed by Center for Humane Technology helps us to assess the home-assistant devices using various human sensitivities such as Emotional, Attention, Sense-making, Decision-making, Social Reasoning and Group Dynamics. We will also be analyzing how the devices engage or elevate the human sensitivities and what action can be taken from us to improvise it.

As we discussed in the current situation, most of the home-assistant devices work on voice-enabled commands given by the user. These devices come embedded with a microphone which is constantly kept on so that they can be triggered to action as soon as the specific command is given to them. [17] Also, these devices need 24*7 internet connection to work and assist us. While they are constantly using the internet, they also keep sending data information to the company's servers so that they can work efficiently. These devices unfortunately record our normal conversations while waiting for any voice command from the user, and upload/exchange the conversation data over the internet. [17] Many of these devices come embedded with such sensors and software which are kept constantly on so that they can work efficiently. But these sensors are so vulnerable that anyone can easily hack it to eavesdrop on the user or anyone can access the data which these devices keep constantly exchanging over the internet. This state/environment where the user knows the devices are constantly monitoring them can lead to stress or fear among the users. Their behavior and actions will be restricted if they know that they are constantly being monitored.

Although these devices keep constantly monitoring the users' environment to assist them as soon as the user commands it, they do not seek much attention from the user. These devices will not assist the user until he/she gives the command to it. Still, these devices can end up consuming users' important time and comfort while they are giving the commands to them. The major problem with these devices is that they either work only with specific phrases given by the company to the user or controlling them with the applications from the smartphone. Users end up wasting the time and stressing themselves out by giving the commands to these devices through specific phrases and still not getting the assistance from it. [18] These devices that do not seek much attention of the user in a whole day end up taking most of it at once when the user tries to command them.

Most of the home-assistant devices usually provide the information, facts, and other daily news to the users on their command. Sometimes, these devices end up being biased while providing such valuable information or news to the user and since the user relies on these devices, it affects the sensibility of the user. Users are not able to sense that the information provided to them is manipulative or fake since they are the ones who purchase these devices, and they end up trusting them. This can lead to affect group dynamics by spreading hatred and outrage among larger groups. These devices also are in constant touch with their company's servers and keep sending the data collected by them. These companies

sell/exchange the data with third-parties to generate the revenue. Third-party companies can analyze the users' emotions based on the data collected by these devices and target them with the advertisements when they are most vulnerable, thus leading to subconscious manipulation of the user. [19]

The home-assistant devices do not follow the informed-consent protocol before retrieving the data of the user, which is also a serious concern in terms of privacy breach. Regulatory bodies come up with the solution as various data regulations, which companies also need to abide by. Companies provide 'Terms & Conditions' to the users before sharing their data to third-party. [20] This solution trying to avoid one ethical issue brings up another one. These 'Terms & Conditions' provided by companies are innumerable (consisting of multiple pages) [19] and written with complicated words [19], which the user finds extremely difficult to read and understand. [20] The user eventually accepts it by agreeing to 'Terms & Conditions' to utilize the service and save time and individual effort. [19] It renders the false sense of security among users and affects the decision made by them.

b) Good clean fair framework

Good ICT:

A good ICT is simply "socially desirable", projects and applications are developed starting from human needs, and the technology is human centered. According to Richard De George: "Computers and information technology should help and serve people and society. Where they do not, they should not be passively accepted" [21]. We know that firstly they created these kinds of smart devices to provide comfort to humans but nowadays the situation is different as too many big companies are in the race of collecting big data from users. We can realize that big data is the new key to create a big business. But that is "not an ethically Good" solution.

People have the right to know about their digital identity, how it is managed, and to have control of its storage and processing, including the right to oblivion [22]. When we use home assistance devices, we fire a command towards it and it reacts based on algorithms, but it also collects data by intelligent tools like what we want, who we are, what are our interests and many kinds of information from those commands given by us. And we don't know how it is stored and how it is going to be used. This is conflicting with this framework and not satisfying Good ICT criteria.

Good ICT must be safe, and this is particularly important for technologies where software (and its fragility) plays a central role [23] [24]. As we discussed above in the current situation section, there might be a sensor failure or algorithm failure. Because of that people have to bear a big loss or it may be risky for human life also. While creating any kind of technology one should consider this kind of risk also, and there should be some solution like auto troubleshooting so we can save human life as well as losses.

We also can think in other dimensions like, big companies are able to collect all the data from us as they have a lot of resources and a high amount of workforce and technology. They use our data to target us and they can earn a lot of money. On the other hand local startups and local stores are not getting customers as they do not have a lot of money and technology. We can see tremendous growth in billion dollar companies and our local store

owners are at risk. This can make an imbalance in the economy also. So this is a very crucial point to think about.

Clean ICT:

A clean ICT is simply environmentally sustainable. To store data generated from home assistance devices cause pollution and consume a lot of energy. ICT power consumption is predicted to balloon to 20% of global electricity demand by 2030, which would mean a greatly increased carbon footprint. Something must be done [26]. Data Centers use an estimated 200 terawatt hours (TWh) each year. This is more than the annual energy consumption of some countries. They contribute around 0.3% to overall carbon emissions, while the information and communications technology (ICT) ecosystem as a whole accounts for more than 2% of global emissions [25].

Other than that, we are generating a lot of e-waste, every second someone is buying a new smart device by replacing older ones. There are very limited recycling processes to reuse older parts. Big companies and national officials throw their waste at other countries to make their own country clean, instead of this they have to find such solutions that are less pollution to the environment. To make this more feasible, we need to find such solutions that take less energy and generate less pollution also. Indeed, the concept of limits has recently been introduced into the ICT domain for investigating the impact and the environmental, material, energy, and social limits of ICT. The area of "computing within limits" is now becoming critical for the future of ICT itself [27].

Fair ICT:

A fair ICT is simply one that is socially acceptable. Among the many vulnerable stakeholders of the ICT world, these members of the workforce are often forgotten. Nowadays mostly located in south-east Asia, every day these workers produce the devices used by the rest of the world. A fair ICT should pay attention to their working conditions, their human rights, dignity, and lives [28]. If we consider the ICT industry in India there are no fixed working hours for employees, they have targets to complete in limited time, so they have to do overtime and they don't get paid for that. Many employees are having stress because of heavy workloads, and many facing physical problems like neck, back or eye problems due to working for hours seated on the same chair. There may be more such issues which should not be forgotten.

After discussing all the three contexts of home assistance devices, we should not exclude positive sides of these devices.

In today’s busy life, we cannot do all the work perfectly and on the correct time, we may forget some work, so this device can be boon for us as we discussed in the benefits section. Moreover, these devices are very much needed for handicapped people and youngsters. These devices provide comfort and ease in day to day life. All the big companies working under the government's privacy preservation rules, so people are less concerned about their personal data to be leaked or used in other ways. So, this solution is widely accepted by society and numbers are still increasing.

c) IEEE Code of Conduct

Although smart-home assistant devices offer huge benefits, comforting people to remotely operate technological devices, it is equally important that these devices respect humans and their sentiments. This concern aligns with privacy of an individual and protection of online private data which is shared with these devices. A smart home connects tens of home devices to the Internet, where an IoT cloud runs various home automation applications. [32] While bringing unprecedented convenience and accessibility, it also introduces various security hazards to users. As mentioned in [32], the targets of the attack are cloud-connected devices which directly communicate with IoT clouds. The attacker's goal is to take control of the device or to monitor/manipulate the data collected/generated by the device. Thus, the attacker has the capability to collect personal information of the user.

The risk of privacy intrusion acts as a major inhibitor to smart home acceptance and adoption. A breach in privacy of users may happen as a result of unwilling information disclosure, and the inability to control the interference of automation systems in private life [30]. Sensors attached in various home assistant devices do the task of motion sensing, thereby tracking physical activities for operating smart devices. While they can be very useful for comfort, entertainment and health related stuff, such devices can be a threat to privacy if attacked by adversaries via hacking. In a TED talk video on online Privacy vs Monetization, Stuart Lacey highlights that Samsung smart TVs were shipped with their webcams and microphones enabled by default, which can be hacked. Thus, anyone could monitor your activities in the bedroom or living room, thereby violating your private space. While apps by such large companies can have data privacy concerns, it becomes difficult for end-users to put faith in most of the applications out there.

Fairly treating people includes not engaging in harassment of any kind, along with proper behavior. Smart home assistant devices should be used in a way which does not affect the emotions of an individual. For instance, some companies rely on electronic monitoring of their employees at work and further justify this act under increasing overall productivity. In this way, by using such technologies, people's privacy at the workplace can be threatened. Furthermore, this can lead to a fear of always being watched by someone and they may lose their focus at work.

Social discrimination due to such technology is also one such concern which needs to be addressed. For example, a user may not wish to use assistive technologies, due to concerns that they will be stigmatized and labelled as vulnerable people [30]. This should not be the case as each individual has rights to use technology of his/her interest. Such stigma can be avoided if people acquire proper knowledge about these smart home devices and learn about various benefits they offer.

Reputation of an individual and social equality are two important ethical concerns related to smart home technology. Financial stability is one such factor in a user's socialization. It may give rise to a threat that only higher-income users may benefit from smart home technology and experience social inclusion in the society of luxury technology holders [29]. Along with this, user confidentiality, access and authentication threats are also one of the main reasons damaging the reputation of an individual [31].

d) Solutions

There are many exciting solutions, which are very useful to preserve users' privacy and other issues which we have discussed above. One and the most effective solution for privacy protection laws made by the EU, In the same way each country has their own privacy protection laws. Any company who wants to start any ICT business must have to follow these rules and if they violate any rule they have to go through legal procedures. Sometimes, they have to pay a big penalty, or their services may stop working in that particular country. For instance, Google has different privacy policy in the EU compared to other countries as the EU changed some rules and Google was not able to follow those rules, so Google had to change its policy. So, this is globally accepted and a very good solution to preserve users' privacy.

There may be new proposed solutions which also help us to get relief from these issues like, A good ICT is designed in accordance with the Participatory Design approach in which users collaborate with designers in joint teams [33]. According to this, consumers should be involved in the design process of any product, as they are going to use it. We can conduct surveys before making any product, and after making products we also conduct surveys by giving these products to some of different users and take feedback. If they find any serious issue we can change it and make a final product which satisfies the needs of users as well as the company. But all the users can not belong to the IT field so they cannot have knowledge about real issues generated by particular products, and they also do not know what challenges companies could face while making products that can satisfy each user's demand. But this can be a great idea that IT employees and users get together and make user friendly products.

Good ICT should also help human beings to use less ICT and find the right balance in time between online and offline [34]. As we discussed in the previous paragraph, we can include users in the design process, that will definitely balance the time one should spend online and offline. Users provide information which can reduce our reliance on particular products.

Users should have access to data, they can delete or modify data according to their comfort to assure their security. We have these options nowadays in outsmart devices as we can turn of our location and other access from any soft wares, but this kind of solution we also need for home assistance device as it always listens our talk, microphones are active 24*7. So it transmits a lot of data to companies which we aren't aware about. And if we delete data from any online account, it is still present at some place that should not happen as we have the right to delete our personal information.

As we saw in the previous paragraph home assistance devices always listen to us whether we want or not. According to Erik, we can build some systems that detect humans, and there are many available also. Using this system we can activate the microphone of the device, this can solve 2 problems. First is we will less worry about unnecessary data transmission to the company and second is sometimes smart devices activate on wrong time because of encountering bugs or any algorithm or sensor failure which is discussed in the current situation part, this can be resolved also.

Moreover, as clean ICT should address challenges by minimizing the extraction of new materials (e.g. by recycling and repairing devices), by reducing considerably the power

consumption of ICT, ensuring the use of renewable energies, and stopping the export of e-waste to Africa and south-east Asia. Each of these measures need the collaboration of a wide range of stakeholders: of users (by improving their purchasing selective criteria), designers (by innovating the ICT supply chain incorporating the reparability-by-design rule), and policy makers (by introducing strict norms for the release of new products onto the market, if they are not recyclable, repairable, and not accompanied by a strict Life-Cycle-Assessment) [36]. So in this area a lot of work is going on and we are able to recycle and reuse products, we also have electric circuits using less energy and doing less pollution.

5. Conclusion

As home-assistant systems become more popular, they are also serving as a wake-up call on what modern technology can do if it is not ethically corrected before being introduced in the market. While these devices support us in a number of ways, we may summarize that they do so in an unethical manner. To conclude, there exist many ethical issues related to home assistance devices that need to be discussed. Additionally, it becomes equally important that these issues are illuminated to everyone who is using these devices in their everyday lives as well as planning to have them in future. Although steps are being taken to solve them, there exist many such issues that need to be solved that are mainly focused on privacy, integrity and confidentiality of a person. Along with this, various factors should be considered to eradicate social stigma related smart home assistance devices. Only then we can say that the technology is completely ideal for the usage by mankind.

.

6. References

1. Clickatell. A guide to home automation and smart home assistants. https://www.clickatell.com/articles/technology/home-automation-smart-home-assistants/ (accessed March 22, 2021).

2. Lacey S. The Future of Your Personal Data – Privacy vs Monetization. TEDxBermuda 2015. https://www.youtube.com/watch?v=JIo-V0beaBw&ab_channel=TEDxTalks (accessed March 22, 2021).

3. Myrstad FL. How tech companies deceive you into giving up your data and privacy. TED Salon: Samsung 2018. https://www.ted.com/talks/finn_lutzow_holm_myrstad_how_tech_companies_deceive_you_into_giving_up_your_data_and_privacy (accessed March 22,2021).

4. Greenwald G. Why privacy matters? TEDGlobal 2014. https://www.ted.com/talks/glenn_greenwald_why_privacy_matters?language=en (accessed March 22, 2021).

5. Patrignani N., Whitehouse D. Slow Tech: Towards and ICT for the Anthropocene Age. Visions for Sustainability; 12: 35-39

6. Edu J., Such M., Suarez-Tangil G. Smart Home Personal Assistants: A Security and Privacy Review. ACM Computing Surveys 2021; 53: 1-36

7. Emily Gorcenski: The Ethics of the Internet of Things | JSConf EU 2017. https://www.youtube.com/watch?v=xLL7Fo_em2E .

8. Kashmir Hill and Surya Mattu. What your smart devices know (and share) about you. TED2018.https://www.ted.com/talks/kashmir_hill_and_surya_mattu_what_your_smart_devices_know_and_share_about_you

9. “Smart Home Market (Smart Kitchen, Security & Access Control, Lighting Control, Home Healthcare, HVAC Control and Others): Global Industry Perspective, Comprehensive Analysis, Size, Share, Growth, Segment, Trends and Forecast, 2016 - 2022”- http://www.zionmarketresearch.com/report/smart-home-market

10. "Smart Home - Worldwide." - https://www.statista.com/outlook/dmo/smart-home/worldwide.

11. “The Internet of Things: a movement, not a market” - https://cdn.ihs.com/www/pdf/IoT_ebook.pdf.

12. IEA (2017), Digitalisation and Energy, IEA, Paris https://www.iea.org/reports/digitalisation-and-energy.

13. Faruqui A., Sergici S., Sharif A."The impact of informational feedback on energy consumption – a survey of the experimental evidence" Energy, 35 (4) (2010), pp. 1598-1608, 10.1016/j.energy.2009.07.042

14. "Avast Smart Home Security Report 2019" - https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

15. Guhr, N., Werth, O., Blacha, P.P.H. et al. Privacy concerns in the smart home context. SN Appl. Sci. 2, 247 (2020). https://doi.org/10.1007/s42452-020-2025-8

16. Center for Humane Technology. Design Guide (Alpha Version). https://www.humanetech.com/designguide (accessed March 25, 2021).

17. Edu J., Such M., Suarez-Tangil G. Smart Home Personal Assistants: A Security and Privacy Review. ACM Computing Surveys 2021; 53: 1-36

18. Hill K., Mattu S. What your smart devices know (and share) about you. TED2018. https://www.ted.com/talks/kashmir_hill_and_surya_mattu_what_your_smart_devices_know_and_share_about_you (accessed March 25, 2021)

19. Myrstad FL. How tech companies deceive you into giving up your data and privacy. TED Salon: Samsung 2018. https://www.ted.com/talks/finn_lutzow_holm_myrstad_how_tech_companies_deceive_you_into_giving_up_your_data_and_privacy (accessed March 25, 2021)

20. Lacey S. The Future of Your Personal Data – Privacy vs Monetization. TEDxBermuda 2015. https://www.youtube.com/watch?v=JIo-V0beaBw&ab_channel=TEDxTalks (accessed March 22, 2021).

21. EU (2019), European Union, Complete guide to GDPR compliance, https://gdpr.eu/

22. De George R.T. (2003) The Ethics of Information Technology and Business, Blackwell Publishing, p.ix.

23. Rogerson S., Gotterbarn D. (1998) The ethics of software project management, in G.Collester (ed.), Ethics and information technology, Delhi.

24. Gotterbarn D. (1992) Software Engineering Ethics, in Encyclopedia of Software Engineering, ed. John J. Marciniak, John Wiley & Sons, Inc.

25. Digitalisation and Energy, https://www.iea.org/reports/digitalisation-and-energy.

26. Gunnar Menzel, Solution architects and designers should consider environmental factors and sustainability while designing equipment.https://www.capgemini.com/2020/01/the-more-sustainable-data-center

27. Workshops on Computing within 38 Limits, LIMITS 2021 -- Workshop on Computing within Limits.

28. OECD (2004) Organization for Economic Cooperation and Development, Illegal Exploitation of Natural Resources in the Democratic Republic of Congo: Public Statement by CIME (Committee on International Investment and Multinational Enterprises), www.oecd.org.

29. Marikyan, D., Papagiannidis, S., & Alamanos, E. (2018). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change. doi:10.1016/j.techfore.2018.08.015

30. Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu, and Yuqing Zhang, Discovering and understanding the security hazards in the interactions between iot devices, mobile apps, and clouds on smart home platforms, 28th USENIX Security Symposium (USENIX Security 19) (Santa Clara, CA), USENIX Association, August 2019, pp. 1133–1150.

31. Chung, J., Demiris, G., & Thompson, H. J. (2016). *Ethical Considerations Regarding the Use of Smart Home Technologies for Older Adults: An Integrative Review. Annual Review of Nursing Research, 34(1), 155–181.* doi:10.1891/0739-6686.34.155

32. Lin, H., & Bergmann, N. (2016). *IoT Privacy and Security Challenges for Smart Home Environments. Information, 7(3), 44.* doi:10.3390/info7030044

33. Nygaard K. (1996) Those Were the Days, Scandinavian Journal of Information Systems, 8(2):91-108.

34. Fasoli M. (2019) Il benessere digitale, Il Mulino. Floridi, L. (2014) The Fourth Revolution. How the Infosphere is Reshaping Human Reality, Oxford: Oxford University Press.

35. The Top 5 Problems with Smart Home Tech and How to Troubleshoot Them, Eric Murrell. https://www.nachi.org/problems-smart-home-tech.htm

36. Andersen O. Hille J., Gilpin G., Andrae A.S.G. (2014) Life Cycle Assessment of electronics, IEEE, https://ieeexplore.ieee.org/document/7046212. Bateson N. (2019) Warm Data, https://norabateson.wordpress.com/2017/05/28/ warm-data.