COMP3041 Professional Ethics in Computing
Topic 3: Ubiquitous Computing

GROUP G

Name	Student ID
Loh Jin Xian	18816763
Bung Jing Quan	18817145
Ahmad Sami Ahmad Hussein	024119
Ezzeddin Nader Ezzeddin Tagiuri	024030
Christopher Lychealdo	20121244

Table of contents

Introduction

Ubiquitous computing is a model in which the handling and processing of data, it occurs using any location, any device, and any type. The presence of computational ability in everyday objects, which is also known with the term “smart objects” allows the possibility to improve human’s life.

There are 3 general ubiquitous computing features: the ability to provide transparent interfaces, the ability to automatically adapt the behaviour of a program based on knowledge of the context of its use, and the ability to automate the capture of live experiences for later recall.

Having the world heavily reliant on different devices used by millions of users ranging from computer to even house appliances. This shows the integrated world we live in. In order to make the devices capable of understanding human, a sensor network is created to collect, process and send data to the cloud. Artificial Intelligence and machine learning are deeply woven into our lives to achieve the ultimate fictionalized use of computing.

Many of us are unaware of just how much our lives are affected by these technologies because they fit so seamlessly into our day-to-day. This seamless integration is made possible by the emergence of ubiquitous computing with the data processing capability of artificial intelligence.

Here are some major ethical and technical aspects of Ubiquitous computing that heavily affected our societies:

- Ethical and unethical privacy penetration
- Ecosystem of the ubiquitous computing
- Artificial intelligence in ubiquitous computing
- The psychological and sociological effects on users in short term and long term.

Privacy and Safety

Unlike in the past when computers were nothing more than large boxes sitting underneath our disks, today's computers come as smartphones, glasses, cars, tablets, fitness trackers, smartwatches, and so on. They are significantly smaller and more powerful than before and due to that, scientist and engineers are looking into new ways of harnessing its power and portability to sense it in our everyday lives. That's where Ubiquitous Computing comes into play.

Although Ubiquitous Computing has introduced new technologies in the areas of communication, healthcare, transportation, etc. These technologies also imposed significant risks when it comes to privacy. Due to its nature, Ubiquitous Computing makes it easy to intentionally or accidentally share personal information of users. Many IOT devices manufacturers and suppliers show little to no regard when it comes to disclosure of personal information. For instance, the US federal trade commission has accused "Genesis Toys", the manufacturer of "smart" kid toys of violating privacy rights and the disclosure of personal information. The smart toy keeps records of all the conversations nearby its location. In addition, it asks children for personal information such as their name, where do they live, favourite meals, etc.

Moreover, according to WikiLeaks, The **CIA** (Central Intelligence Agency) along with the MI5(United Kingdom Spy Agency) has developed a cyber-attack that is capable of activating the microphone in the Samsung smart TVs without the user consent, allowing them to remotely record conversations. What is more concerning than this is that if the **CIA** is capable of violating our privacy and gather sensitive data from users, any cyber-criminals or terrorist would be able to do the same and unfortunately the **CIA** has not taken any action towards solving this issue.

While having an IP-enabled toaster may make it easier to prepare breakfast, it also makes it easier for hackers and malicious actors to steal passwords, financial data, health information, and other sensitive materials. IOT devices recently were involved in the few of the largest so called "distributed - denial of service attacks" which are basically cyber-attacks that flood websites with enormous amount of data until they crash. For instance, in late 2016, series of distributed-denial of service attacks targeting systems operated by domain name system provider "Dyn". The Dyn attack caused the major internet platforms and services unavailable to a big portion of users in North America and Europe. It turned out that the vulnerability of IOT devices and the easiness of bypassing its security protocols was the leading cause of this attack.

Besides, IOT devices can be dangerous by themselves. In 2015, “fiat”, the Italian automobile manufacturer recollected around 1.4 million vehicles after a group of researches figured out a way to bypass the “smart” car system protocol and remotely control breaks, steering wheel, temperature, etc.

A prime example when it comes to concerns over violation of privacy is ‘Google Street’ since its launch in 2007. Google street is a technology which provides panoramic view of most of the streets in the world. Due to this, many places including homes can be clearly visible in the map. In fact, there is a couple in Pittsburgh who sued google because they found that their home is evidently visible in google maps. They claimed that this made extremely uncomfortable and cause them “mental suffering”. Also, there is a woman who claimed that she found naked images of her daughters while they were playing in their paddling pool. Google has made an initiative to solve google street privacy issues and they came up with a solution that they claim it solved the issue but in reality, it did not. The solution was to blur people’s faces and car license plates.

Ecosystem

Ubiquitous computing which has been a common technology nowadays serves magnificently to the community. Since there are tiny Internet of Things (IoT) devices that can work seamlessly and all day for individuals, visual clustering has been reduced and redundant daily task need to be done can be mitigated. Such application of technology significantly shows the improvement of individual’s lifestyle and possibly boost performance on other tasks.

Smart technology such as Smart Home is the most conspicuous, trending terms that can be related to these criteria. According to Gfk smart home study’s, 78% of global consumers agreed on smart home concept. Such technology is still rapidly growing all over the globe. On the same time, technical and ethical issues on smart technology are arising accordingly as well.

The service integration is one of the technical issues in such field. Electronic devices from different brands or types construct a complex ecosystem, causing one may find difficulty on pairing up those devices to work as a single service. Not all the manufacturing companies are willing to provide a universal Application Programming Interface (API) for programmers to integrate the services due to business purposes. In addition of no proper IEEE standards and authority laws to control the monopoly in the prior of time, users are forced to buy the products from the same company to experience such restricted service.

This problem can be solved using a third-party software to give commands to specific application to control the desired devices such as If This Then That (IFTTT) or Google Home Assistant. However, the solution leads to the next issue which is the reliability of the services. Since all services is interconnected into one software, failures of such mesh-liked network at the vital node (such as servers) has a high chance of taking down the whole services. This condition could be completely virtualised by an incident that IFTTT leaved users in the dark due to its server, which sat in Amazon Web Service (AWS), went down unexpectedly (Murgia, 2017). Despite of living in the bad experience on the service, users are forced to accept the service they set up.

Next, repair rights on those ubiquitous computing devices has been on the spotlight lately. As per observation, warranty stickers are usually noticeable right above the screw hole of the devices especially mobile phones and gaming consoles. The reason given by the manufacturing companies involving this deed is to avoid third-party services from opening the devices and repair themselves. Therefore, users have to send their broken devices to the related companies for repairs, which costing them a lot more money compared to the third-party service as well as time. However, as stated in the 1975 Magnuson-Moss Warranty Act, no manufacturer is allowed to put repair restrictions on a device which is still under warranty period (Gault ,2018). As a result of such unethical means, in United States, several well-known companies like Microsoft, Apple, Sony, Nintendo received warning letters from Federal Trade Commission (FTC) to take down the warranty stickers (Mills, 2018).

Finally, the culture of subscription-based system has also been popularised compared to one-time-purchase systems. Instead of asking users to buy the service at once, users are forced to subscribe for the service with certain pricing methods, such as monthly or annual payment. In the future, the “per per use” culture will eventually overtake the lead and the users are forced to follow it instead of having options to select for the services.

Artificial Intelligence

With the introduction of pervasive computing devices, one of the ethical issues faced by the majority of the population is that ubiquitous devices are ideally suited for covert operation or illegal surveillance. Having sensors that gather information about people without being noticed can be a threat to personal privacy. Although privacy concern has been an old-age issue with the world wide web, ubiquitous computing is more dramatic in terms of the coverage and types of data being collected (e.g. location, health, habits, movement etc), thus making anonymity of the user harder to maintain. Nowadays, most companies decided to create artificial intelligence that can be scaled to all kind of products. For example, an artificial intelligence created by Google called “Google assistant” is designed to be used in mobile phones, smart speakers, smart televisions and smart cars.

The ultimate goal of these commercial companies is to build a general artificial intelligence that can be summoned at anytime and anywhere, turning it into the most useful utility in people’s daily lives. Great convenience also comes with great sacrifices where the users are required to give up their privacy to realize the potential of a general artificial intelligence. All these personal data are collected to empower the artificial intelligence to learn the daily routines of a user more accurately like what he likes, what he eats, what he listens and what he does normally etc without the need for the user to manually input their personal preferences.

There are countless examples of ubiquitous computing devices in the 21st century, for example, Apple watch, Amazon echo speaker, Fitbit fitness tracker, Tesla self-driving car etc. To illustrate how ubiquitous device works in our daily lives, Amazon echo speaker will be used as an example. Amazon echo speaker is one of the hands-free speakers (or smart speaker) that are available in the market. The hands-free speaker gives the user the ability to use their voices to control the device. This is possible thanks to the state-of-the-art technology equipped inside the speaker like microphones that feature enhanced noise cancellation and far-field voice recognition which boost the coverage of the user's voice.

The Amazon echo speaker also has their own proprietary artificial intelligence system named "Alexa" that can process the commands that the user had made and carry out the required tasks. However, Amazon echo speaker needs to be listening to its environment at all time for the voice command feature to work. By giving up the user's privacy, the speaker is able to play music, provide information, deliver news and sports scores, tell you the weather, control your smart home and even allow the users to order products they've ordered before on Amazon website (Britta & Dan, 2018). Besides that, Alexa is always learning from the user and will adapt to their speech patterns, vocabulary, and personal preferences.

According to the survey done by voice.ai bot website, the total reach of smart speakers in the United States is 47.3 million out of the total population of 252 million, which is quite high given the fact that the first smart speaker which is Amazon Alexa speaker, has only been introduced for 3 years (Kinsella, 2018). In just 3 years, the population has adapted to the convenience provided by smart devices and instantly incorporate them into their lives. To put things into perspectives, it took a long 13 years for television to reach an amount of 50 million users where smart speakers only took 2 years to achieve this target (Perez, 2018).

Psychological, Societal, and Individual Impact

The smart technologies are reaching more and more customer. One example is the adoption of smart speakers, which has reached 50 million units at the end of 2017 and forecasted to reach 100 million units by the end of 2018 (Knight, 2018).

Smart devices have a lot of uses. The smart speakers, particularly, can be used to assist humans in daily activities. Many users use it daily, with 25% users use smart speakers to set an alarm, 33% uses it to ask a question, 41% uses it check the weather, along with other uses (Kinsella, 2018). The data shows that smart technologies have become more integrated than ever into humans' life.

Smart technologies can also assist people with disabilities and deficiencies. Smart locks, doorbells, and the speakers are some of the technologies that could help assist people with disabilities and deficiencies (The Tipping Foundation, 2018). With these integrations starting to become part of our daily activities, studying the effects on our society and psychology seems important.

Along with the smart objects' possibilities to enhance human's life, from reducing stress by promoting more control, to providing more independence, there are possibilities that these devices might alter social behaviour and abused by irresponsible parties.

Two of the main issues in smart products are the issue of privacy and personal information, and effective wellbeing (Pillan & Colombo, 2018). When a device is connected to the internet, it is vulnerable to attacks. This means that it is possible that everything recorded on a smart speaker can be obtained by other parties, as well as the device being hacked or abused, which might harm the owner of the device. Jarosciak stated that he believes that regarding to data ownership and security, smart speakers are susceptible to cyber-harassment and cyber-bullying (Jarosciak, 2017). Cyber-bullying and harassment is more difficult to deal with as it could be public and spreads quickly.

House is where people grow and establish relationships, search for affection with people, and build social experiences which build behaviour and lifestyle (Pillan & Colombo, 2018). The use of smart objects, such as smart speakers, where the interactions between human and the device is mostly through voice communication, has a possibility to deter the opportunities for individuals to experience social interactions in a house. Without any parental control, children are susceptible to discover things that might not be suitable for their age, and parents' role to provide answers to their question is diminished.

Although the smart technologies adoption rate is rising, a survey shows that some customers are hesitant to own a smart device (Richter, 2017). Worries about hackers misusing the device, the speakers are always listening, and not having enough knowledge about the speakers are some of the top reasons. This means privacy is a concern, as it might affect the users' psychological state and possibly their social life.

In a CNBC article on the effects of smart assistants, Lindholm stated her fears on the possibility of kids considering smart assistants as real people, using them to get information on things that they would ideally discuss with their parents (D'Onfro, 2018). Brett Gaylor, through his video with The National Film Board of Canada, showed him opening the playback of what his child asked to Google Voice Command, and noticed that his child and the smart assistant developed a form of relationship which can be considered as intimate (Gaylor & Pasemko, 2017).

Considering the benefits and risks, along with its growing adoption rate, education and standards on ubiquitous technologies are substantial to ensure that psychological and societal aspects are not altered in the wrong direction through use of these technologies.

Conclusion

Even though having our devices interconnected creating a whole ecosystem which proves to be very convenient, companies may prove to abuse such ecosystem with giant business models forcing users to consume or rely on many unnecessary services to get full functionality of one device. To be worse, by having multiple devices connected and reliant on each other in a smart ecosystem, this will create an unstable ground for the user's privacy as hacking or breaching one device may mean that all have been compromised. In the end, users will end up agreeing to many regulations instilled by the providers of the services or devices which may sell or use their information.

Artificial intelligence devices that integrate into our homes have full monitoring on our daily activities and may send that sensitive information to companies that use that information also. The main issue is that the modern era is heavily reliant on these devices and makes such commodities into necessities, giving little to no choice for users but to adopt the decisions made by the suppliers.

Regulation of these systems must happen to ensure a healthier and safer future for users. A governing body must be established and fulfil set protocols which look for the safety above all else. Users must have the ability to make choices that do not hinder their experience but rather may not get the full experience by not subscribing to such systems. Allowing companies to abuse data of users gives uncontrolled power with little restrictions to what may be applied in the future. The connection of these devices will increase and through that, users and companies must have a healthy relationship that benefits both while sustaining a balance in business, connectivity of these systems, data, and usage.

From the social perspective, these devices are supposed to connect us together, though they have proven to make us more apart, ironically. The solution to this issue would be awareness through education and media. Another practical means of raising this awareness would be through parenting, it is a stronghold for raising the next generations, especially when technology will only progress and ubiquitous computing will continue to engrave itself into our lives.

(2987 words)

References

Augusto, J. C. (2007). Ambient Intelligence: The Confluence of Ubiquitous/Pervasive Computing and Artificial Intelligence. *Intelligent Computing Everywhere,* 213-234. doi:10.1007/978-1-84628-943-9_11

Britta, O., & Dan, G. (2018, September 18). What is Alexa and what can Amazon Echo do? Retrieved from https://www.pocket-lint.com/smart-home/news/amazon/138846-what-is-alexa-how-does-it-work-and-what-can-amazons-alexa-do

D’Onfro, J. (2018, January 14). As Apple gets slammed for addictive smartphones, experts are optimistic about the Amazon Echo and Google Home. Retrieved from https://www.cnbc.com/2018/01/14/effect-of-smart-assistants-like-amazon-echo-google-home-on-kids.html

Gault, M. (2018, April 10). FTC Says 'Warranty Void If Removed' Stickers Are Bullshit, Warns Manufacturers They're Breaking the Law. Retrieved from https://motherboard.vice.com/en_us/article/ne9qdq/warranty-void-if-removed-stickers-illegal-ftc

Gaylor, B., & Pasemko D. (2017). OK Google [Video file]. Retrieved from https://vimeo.com/245992513

How Ubicomp Is Influencing Big Data and AI. (2017, July 26). Retrieved December 2, 2018, from https://insidebigdata.com/2017/07/27/ubicomp-influencing-big-data-ai/

Jarosciak, J. (2017, March 29). Social and Ethical Concerns of Smart Voice-Enabled Wireless Speakers [Blog Post]. Retrieved from https://www.joe0.com/2017/03/29/social-and-ethical-concerns-of-smart-voice-enabled-wireless-speakers/

Jeffrey, W. (2017, November 06). Top 7 things you need to know about ubiquitous computing. Retrieved December 2, 2018, from http://www.monitis.com/blog/top-7-things-you-need-to-know-about-ubiquitous-computing/

Kinsella, B. (2018, March 21). Data Breakdown, How Consumers Use Smart Speakers Today. Retrieved from https://voicebot.ai/2018/03/21/data-breakdown-consumers-use-smart-speakers-today

Kinsella, B. (2018, March 07). Us-smart-speaker-total-audience-reach-FI. Retrieved December 2, 2018, from https://voicebot.ai/2018/03/07/new-voicebot-report-says-nearly-20-u-s-adults-smart-speakers/us-smart-speaker-total-audience-reach-fi/

Knight, S. (2018, July 9). Smart Speaker Adoption to Surpass 100 Million by Year's End. Retrieved from https://www.techspot.com/news/75423-smart-speaker-adoption-surpass-100-million-year-end.html

Mills, C. (2018, May 02). Sony, Microsoft, and Nintendo have 30 days to kill warranty stickers or the government will sue. Retrieved from https://bgr.com/2018/05/01/warranty-sticker-right-to-repair-ftc/

Montag, A. (2018, September 10). Here's what people actually use their Amazon Echo and other smart speakers for. Retrieved December 2, 2018, from https://www.cnbc.com/2018/09/10/adobe-analytics-what-people-use-amazon-echo-and-smart-speakers-for.html

Murgia, J. (2017, August 09). Smart home fails: When technology goes wrong. Retrieved from https://www.androidpit.com/smart-home-fails-when-it-doesn-t-quite-go-right

P. (2017, August 16). What are Some Examples of Ubiquitous Computing and Convergence? Retrieved December 2, 2018, from https://www.plengdut.com/convergence-and-computing-ubiquitous-of-examples-some-are-what/10927/

Perez, S. (2018, March 07). 47.3 million U.S. adults have access to a smart speaker, report says. Retrieved December 2, 2018, from https://techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says/

Pillan, M., & Colombo, S. (2017, September 6). Will smart homes improve our lives? A design perspective towards effective wellbeing at home. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/14606925.2017.1352769?needAccess=tru&

Richter, F. (2017, October 12). Google Home Issue Fuels Smart Speaker Privacy Concerns. Retrieved from https://www.statista.com/chart/11466/reasons-not-to-buy-a-smart-speaker/

Sharon, S., Beth, T. A., & Margaret, R. (n.d.). What is pervasive computing (ubiquitous computing)? - Definition from WhatIs.com. Retrieved December 2, 2018, from https://internetofthingsagenda.techtarget.com/definition/pervasive-computing-ubiquitous-computing

The Tipping Foundation. (2018, June 5). Ways Smart Home Technology is Benefitting People with Disability. https://www.tipping.org.au/6-ways-smart-home-technology-is-benefitting-people-with-disability/

UK Smart Home Statistics in the UK from GFK. (2016, June 23). Retrieved from https://www.dataselect.com/uk-smart-home-statistics/