Government Subsidy for Internet of Things (IoT) Service

Tommy Oh

301544525

CMPT 105W: Social Issues and Communication Strategies in Computing Science

Harinder Khangura

koa18@sfu.ca

October 28, 2022

Audience: I am writing to persuade Environment and Climate Change Canada to support/subsidize people who want the Internet of Things environment.

Government Subsidy for Internet of Things (IoT) Service

Introduction

In the 21st century, various technologies have permeated people's lives, increasing productivity and providing convenience. Correspondingly, Artificial Intelligence (AI) has advanced through the decades. With the advancement of AI, the concept of a smart home system has attracted people's attention. The Internet of Things (IoT) industry has expanded into several areas, such as "home automation, roads, farms, factories, and power plants" (Elkanishy et al., 2021). Through home automation, users remotely observe and control their homes on their smartphones and laptops. Primarily, Google, Apple, Samsung and Amazon are companies that create hub platforms that connect to IoT devices. For instance, Smartthings, developed by Samsung, is one of the hub apps that is available for consumers today. Using AI technology with home automation, smart home systems are able to collect data from users and provide the best results based on an algorithm. Various technologies have grafted into the Internet of Things (IoT). Already IoT services offer beneficial features for people and industries, such as security and energy saving. There are several companies and people that are trying to adapt IoT services to their environment. Along with the growth in IoT, security and privacy concerns are still being addressed. However, one of the most significant hurdles to the development of this industry is its prohibitive cost to the average consumer. Thus, the government should subsidize Smart Home devices to enable more people to adopt them into their daily lives because of the added efficiency, health benefits, and environmental benefits.

Security Issues - Opposite

Despite the benefits of smart technology, many critics argue that IoT devices lack adequate security. Smart devices, such as smartphones and IoT devices, start to receive user data

to develop the program. IoT systems already permeated people's lives several years ago. IoT systems collect users' data through several services, such as home monitoring, appliance control, and home security (Budi et al., 2020). Data collected through IoT devices is sent to service providers, and during this process, data is exposed if the system security is not reinforced to hacking. In this way, security in devices, especially IoT systems, is essential because the data that service providers collect is their responsibility to use. However, they do not take any responsibility if the data is leaked. The information that has been exposed can be used incorrectly by hackers. For instance, hackers can create a new bank account or get loans using people's data. IoT devices are based on interconnection systems; thus, one criticism is that if one is vulnerable to hacking, almost every connected device is exposed to hacking. Software developers are working on analyzing how to secure data from hackers (Tabrizi et al., 2019). Although software developers explore what to work on and develop techniques for security to prevent hacking, people still question system security (Hwang, 2015). While data security is a present risk in IoT devices, it is also an area that is constantly growing and developing. More specifically, according to the chart from Statista (2022), IoT security rates in tech companies have increased since 2019 and are expected to increase from 39 percent to 47 percent by 2023 (figure 1). This data highlights that system security in IoT services is improving every year. Although the current system security level is not entirely able to protect users from hacking, it clearly shows that it is a problem that has been identified, and work continues to improve it every year.

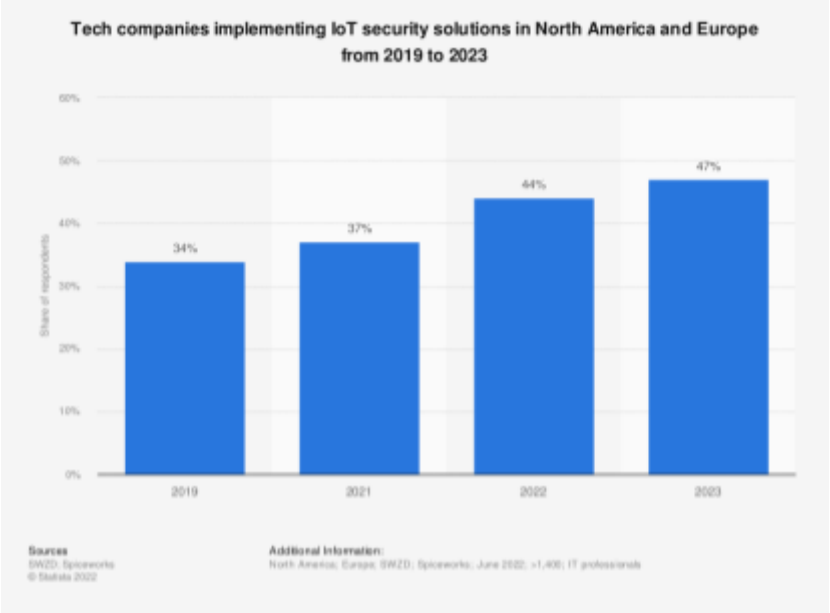

Figure. 1. Tech companies implementing IoT security solutions in North America and Europe from 2019 to 2023

Privacy Issues - Opposite

In addition to security concerns, people's privacy is also a concern as technology develops. Smart devices such as IoT collect data from users for machine learning to develop programs to provide better service. As more devices start to collect personal data from users, people become more nervous about privacy. In IoT devices, the system uses sensors to collect data, which can be private. According to the chart by Statista (2021), the rate of people who are very concerned is 54 percent, and the rate of people who are not concerned about privacy issues is 12 percent, which shows significant differences (Figure 2). This data chart illustrates that most people are still highly concerned about privacy. The biggest problem is that users are unaware of when IoT devices collect data. Users should be informed when the data is collected. There are already many prototypes that are suggested. One of them is reporting a notice to users through their phones. For instance, when people enter a mall, there are surveillance cameras are installed for security purposes. Although surveillance cameras are installed for security, devices collect

personal data, such as the faces of people and the license plate numbers of cars, without people's consent. The proposal suggests that open environments that use IoT services, such as malls, can inform people that IoT services are present and warn them that devices may collect personal data through phones using beacons (Chow, 2017). The alert informs people who are sensitive about privacy and increases a sense of security.

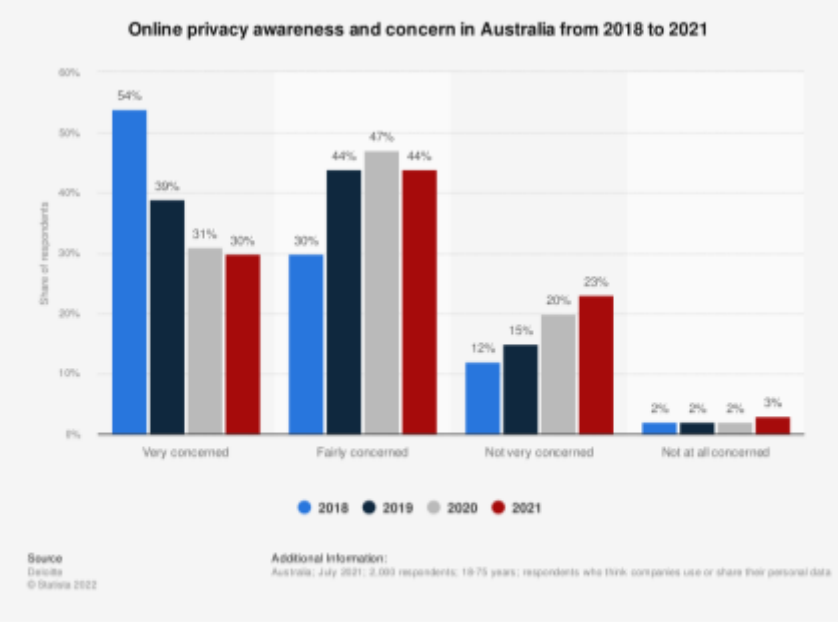

Figure. 2. Online privacy awareness and concern in Australia from 2018 to 2021

Why government should subsidize

Despite the many advantages of IoT devices, the cost is a prohibitive factor. IoT devices have an extensive price range. Some devices are less than a hundred dollars, but most, such as smart lights and IoT home appliances, are worth more than hundreds of dollars. People need to purchase several devices to create a comfortable and smooth service. According to the chart from Statista (2018), customers from several industries, including people who use IoT devices at home, feel financial pressure to adapt. Although IoT services support various technologies, devices have yet to be adopted accessibly into more industries because of money. Government

subsidies can resolve this financial pressure, similar to how they have with electric cars. Similar to the assistance for electric vehicles, there is a need for financial support for people who want to purchase IoT devices. After the government announced the subsidy program for electric cars, the number of electric vehicles increased yearly. According to Statistics Canada (2021), the registration rate of Zero-Emission cars has increased by 0.6% in a year (Figure 3). People who try to purchase a new vehicle can consider purchasing an electric car because of financial support. Following similar reasoning, people who would like to adopt IoT systems into their environment can receive rebates or subsidies from the government, which results in higher rates of adaptation.

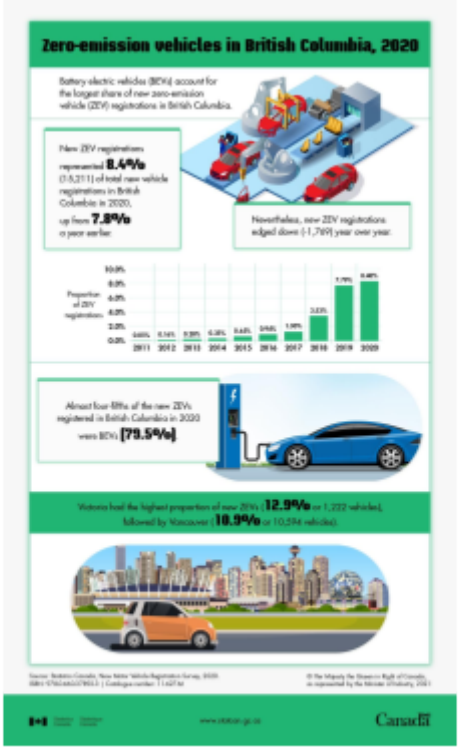

Figure. 3. Zero-emission vehicles in British Columbia, 2020

Energy Saving

One of the reasons that the government should subsidize such an incentive is that global warming is one of the most significant and pressing issues in the world. Several governments

have started investments to prevent global warming. The critical key to stopping global warming is saving energy and using it efficiently. Energy savings is one of the key features that IoT systems support. According to the chart from Statista (2018), 46 percent of IoT users acknowledge that one of the advantages is energy saving (Figure 4). IoT systems allow users to observe their energy consumption, such as how the energy is used in their homes or companies and how to use it more efficiently. Smart thermostats, smart lights, and smart environmental sensors play significant roles in energy saving. Smart environmental sensors collect data about the environment, such as “humidity, temperature, carbon monoxide, [and] smoke presence” (Metallidou et al., 2020). Based on the data collected by environmental sensors, smart thermostats choose how to save energy efficiently through the company's algorithm. One famous thermostat on the market is the Nest thermostat created by Google. Users receive a “Nest Report" that specifically reports how much energy the smart thermostat saves every month. Also, smart lights are able to be controlled remotely, enabling people to manage their lighting in the house when they are out of the home. Smart light companies, such as Phillip Hue, have a feature to turn off all lights when the users leave home based on the Global Positioning System. Controlling lights remotely reduce any wasted energy because of lighting. According to Metallidou (2020), IoT-based designs can increase “power efficiency up to 82.77% a day and minimize carbon emissions by cancelling the use of fluorescent and static power control” (p. 63682). Thus, IoT systems benefit the goal of energy savings, which is the primary goal for the world.

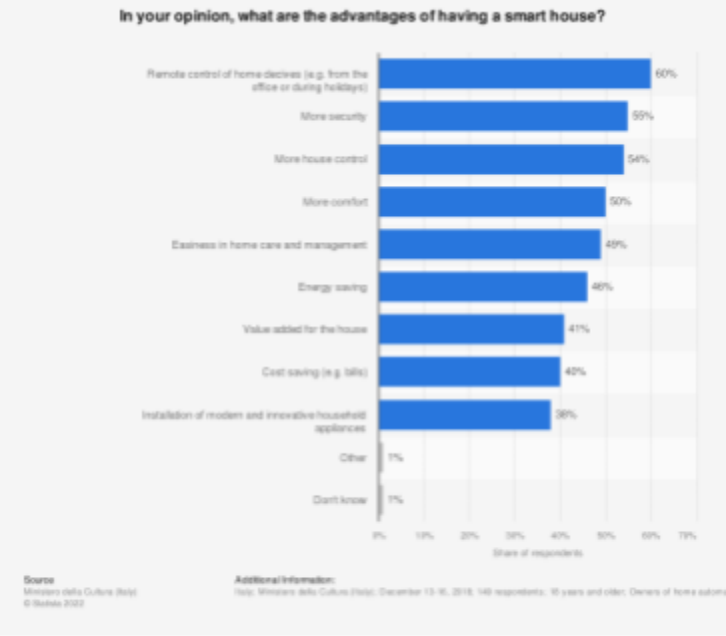

Figure. 4. In your opinion, what are the advantages of having a smart house?

Positive Impact on People's lives - Security

There are several IoT services that offer greater security in people's lives. According to the chart by Statista (2021), the most significant popular IoT appliances are smart speakers that connect IoT devices and security (Figure 5). Surveillance Cameras and smart door locks are devices that people use for security. Both devices can be controlled by smartphones and laptops through smart devices. Smart surveillance cameras support facial recognition and save videos into cloud services. The features that surveillance cameras support can provide reasonable security to people. Facial recognition can be used to identify which people are entering their homes or businesses. It makes people feel safer. Another feature is the recording video system that records and captures what happens at a specific time (Singh et al., 2010). The recorded videos can be used as evidence if something happens, such as at crime scenes. Smart door locks are devices that can be used at houses. Door locks that people normally use at their houses use keys to unlock them. It does not provide perfect security to people. Everyone who has the key,

even duplicates, can access the houses, which makes the house vulnerable (Pandit et al., 2017). To improve security door locks, digital door locks are beneficial to provide observable safety. It allows remote control and leaves a log of which people came. If people are not at home, they still have access to environmental security and are able to observe. With the combination of surveillance cameras and smart door locks, people create the perfect security system of their choosing. The IoT system has endless possibilities of potential that can increase the quality of people's lives.

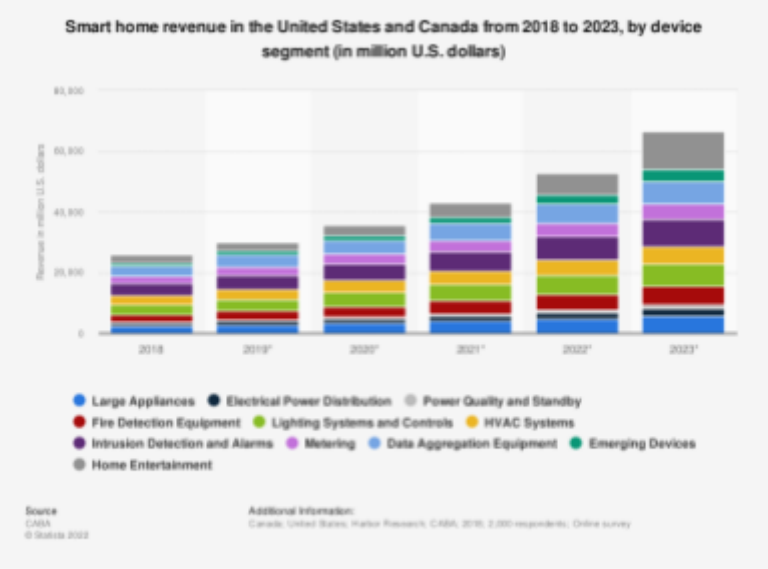

Figure. 5. Smart home revenue in the United States and Canada to 2023, by device segment (in million U.S dollars)

Future Potential - Health

Wearable devices such as smartwatches are also part of IoT devices. Wearable devices, such as the Apple watch, contain several wireless sensors that check people's health. The watch can observe information, such as how many calories the user uses, and can call falling if detected. Wearable IoT devices have unlimited potential in several industries. Wireless Sensor Network (WSN) in wearable IoT devices are generally used in healthcare environments to monitor people's biological and psychosocial signals (Wu et al., 2019). These services can

improve people's quality of life when they are working in industrial workspaces, especially those who work both inside and outside. Safety is one of the keys to the industrial workspace. Especially in the outside environment, there are several factors that can be harmful to humans, such as UltraViolet, ozone, and carbon monoxide. In order to prevent people from being hurt by these factors, industrial workers should be monitored through wearable devices. By using wearable IoT devices, people can work in a safer environment, and IoT devices can track workers' health and prevent any risks. Although it is still a prototype, it will be great for both the environment and people if the system is adapted.

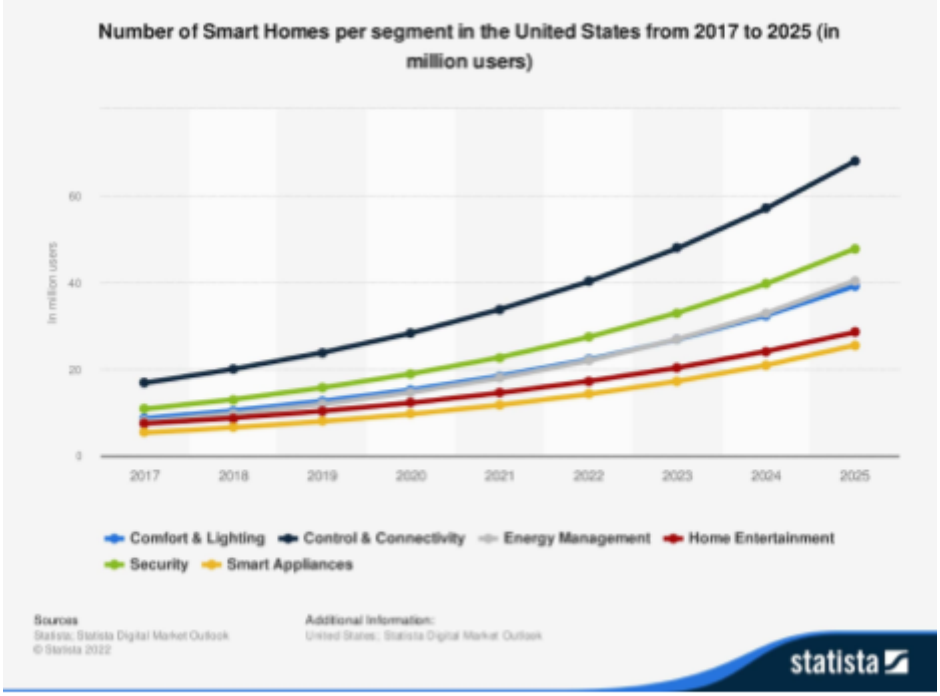

Figure. 5. Number of Smart Homes per segment in the United States from 2017 to 2025 (in million users)

Conclusion

Overall, Smart home technology is one of the fastest-growing industries in the 21st century. The introduction of smart home technology to society has changed the way that people live their lives. Smart home automation is designed to help people live efficiently. Sensors and

IoT devices collect lifestyle data from people and operate efficiently. People are allowed to control their homes remotely by controlling temperature through smart thermostats and lights through smart bulbs. However, the security and privacy of users are still a concern to many IoT users with Smart devices in their homes. Yet, these are issues that have been identified and that are continuing to improve. These issues do not outweigh the notable benefits of convenience, health and energy efficiency that Smart devices offer to their users. Unfortunately, the cost of smart home devices is broad, and the price often comes as a burden to people who want to purchase them. In order to expand the usage of smart homes, the government should assist people and support them.

Acknowledgement

I acknowledge and appreciate Monir Fathalla for checking my persuasive essay.

References

Budi, A., Fitriyah, H., Setiawan, E., Primananda, R., Maulana, R., (2020). Distributed Rule Execution for Smart Home System. SIET '20: Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology. November 2020. Pages 183–189. https://doi.org/10.1145/3427423.3427458.

CABA. (2019). Smart home revenue in the United States and Canada from 2018 to 2023, by device segment. [chart]. Statista. Retrieved November 18, 2022, from https://www-statista-com.proxy.lib.sfu.ca/statistics/1130363/smart-home-revenue-in-the-united-states-and-canada-by-device-segment/

Chow, R. (2017). The Last Mile for IoT Privacy. IEEE Security & Privacy, vol. 15, no. 6, pp. 73-76, November/December 2017, doi: 10.1109/MSP.2017.4251118.

Deloitte. (2021, November). *Online privacy awareness and concern in Australia from 2018 to 2021* [chart]. Statista. Retrieved November 18, 2022, from https://www-statista-com.proxy.lib.sfu.ca/statistics/1202987/australia-online-privacy-awareness-and-concern/

Elkanishy, A., Furth, P., Rivera, D., Badawy, A. (2021). Low-overhead Hardware Supervision for Securing an IoT Bluetooth-enabled Device: Monitoring Radio Frequency and Supply Voltage. ACM Journal on Emerging Technologies in Computing Systems. Volume 18. Issue 1 January 2022. Article No. 6pp 1–28 https://doi.org/10.1145/3468064

European Commission. (2021, June). *Most important barriers to the entry or the expansion of the Internet of Things (IoT) market in Europe in 2020* [chart]. Statista. Retrieved November 18, 2022, from https://www-statista-com.proxy.lib.sfu.ca/statistics/1283899/europe-iot-market-barriers/

Hwang, Y. (2015). IoT Security & Privacy: Threats and Challenges. IoTPTS '15: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. April 2015. Pages 1. https://doi.org/10.1145/2732209.2732216.

Metallidou, C., Psannis, K., & Egyptiadou, E. (2020). Energy efficiency in smart buildings: IoT approaches. *IEEE Access, 8*, 63679-63699. 10.1109/ACCESS.2020.2984461

Ministero della Cultura (Italy). (2018, December). In your opinion, what are the advantages of having a smart house? [chart] Statista. Retrieved November 18, 2022, from https://www-statista-com.proxy.lib.sfu.ca/statistics/964908/opinion-on-home-automation-advantages-in-italy/

Morrison, D. (2021). This infographic highlights key findings from the New Motor Vehicle Registration Survey in British Columbia for 2020. *Government of Canada, Statistics Canada*. https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2021029-eng.htm.

Pandit, V., Majgaonkar, P., Meher, P., Sapaliga, S., Bojewar, S. (2017). Intelligent Security Locks. 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017, pp. 713-716, doi: 10.1109/ICOEI.2017.8300795.

Singh, S., Dunga, S., Mandal, A., Shekhar, C., Vohra, A. (2010). Real-time Object Segmentation in Smart Camera for Remote Surveillance Scenario. 2010 International Conference on Advances in Computer Engineering, 2010, pp. 360-362, doi: 10.1109/ACE.2010.88.

SWZD. (2022, October). *Tech companies implementing IoT security solutions in North America and Europe from 2019 to 2023*. Statista. Retrieved November 18, 2022, from https://www-statista-com.proxy.lib.sfu.ca/statistics/1301970/iot-security-solutions-in-na-and-europe/

Tabrizi, F., Pattabiraman, K. (2019). Design-Level and Code-Level Security Analysis of IoT Devices. ACM Transactions on Embedded Computing SystemsVolume 18 Issue 3 May 2019. Article No.: 20pp 1–25. https://doi.org/10.1145/3310353.

Wu, F., Wu, T., Yuce, M. (2019). 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 87-90, doi: 10.1109/WF-IoT.2019.8767280.