**EG2401A: Engineering Professionalism**

**Next-Generation Connected Systems and Technologies**

****

**Tutorial Group T309 - Project Sub-Group 3**

Gede Arya Chandradhana (A0200704Y)

Goh Kheng Xi, Jevan (A0199806L)

Lock Mei Lin (A0204751M)

**Faculty of Engineering**

**National University of Singapore**

Contents

[1. Overview of Next-Gen Connected Systems 3](#_Toc86233605)

[2. Connected Vehicles 4](#_Toc86233606)

[2.1Latency and Connection Stability of Connected Vehicles 4](#_Toc86233607)

[2.2 Cyberthreats 5](#_Toc86233608)

[2.3 Solution 6](#_Toc86233609)

[3. Home Security 8](#_Toc86233610)

[3.1 Ethical Dilemmas 8](#_Toc86233611)

[3.2 Solution 10](#_Toc86233612)

[3.3 Consequences on Future Generations 12](#_Toc86233613)

[4. Health Trackers 13](#_Toc86233614)

[4.1 Storage and Handling of User’s Health Data 14](#_Toc86233615)

[4.2 Ethical Dilemmas Regarding Health Data Privacy 14](#_Toc86233616)

[4.3 Solution 19](#_Toc86233617)

[References 20](#_Toc86233618)

Honours Pledge………………………………………………………………………………………..23

# 1. Overview of Next-Gen Connected Systems

Developments in the latest sensor networks and telecommunication have given rise to the emergence of interconnected systems, which lays the foundation for the Internet of Things (IoT). IoT opens the gateway to improve IoT has been prevalently used both at the individual and professional levels [1] [2]. Innovations in IoT enable individuals to access their personal information much easier and control their environment with such ease. In particular, IoT has improved the living standards of individuals through innovative connected systems, such as e-health and smart homes [1] [2]. On the contrary, innovations in IoT enable industries to automate manual processes and scheduling. Notably, IoT has helped many industries such as automation, logistics, and smart supply chain [1] [2].

The demand and usage of smart connected systems have been increasing in recent years, and it is projected to continue rising in the future. According to Cisco, around 500 billion devices would be connected to the internet [1]. Other than smartphones, connected vehicles also make up the majority of IoT devices. It is reported that there would be a substantial increase, around 67-90%, of vehicles that will be connected globally with the internet [1]. This shows that **connected vehicles** would be a great contributor to the IoT market and its ethical dilemmas should not be neglected.

One of the main strengths, but also issues regarding connected technologies is their capabilities to store users’ data. Two of the biggest concerns regarding the smart device’s capability to store end-user’s data are privacy and security of user’s data [1]. Such systems are susceptible to hacking from unintended parties and data stored could also be used for companies for other purposes. Although there have been breakthroughs to enhance the security of such systems, we would focus on the ethical dilemmas regarding storing users’ data and their security in the case of a data breach, in particular, smart systems that relate to people’s daily lives such as **health trackers** and **home security systems**.

Health trackers and home security systems have similar dependencies, which is that both depend on data. As their problems are similar, we will change how we approach each case. For home security systems, we will examine in depth regarding the security of these data-driven systems using real-life examples and analyze them using the ethics decision flow chart. On the contrary, for health trackers, we will be analyzing some common real-world situation and create a possible scenario regarding data storage and data privacy violation and putting them into an ethical line diagram. The analysis will also be carried out using the ethical theories we have learned.

# 2. Connected Vehicles

A connected vehicle is one that can connect over wireless networks to nearby devices. For example, the navigation system of a car is connected to the Global Positioning System (GPS) network. When there are accidents or other disruptions on the road, the navigation system can plan a new route to the destination to avoid these disruptions. Another example of a connected vehicle is the Baidu Apollo integrated AI system that is capable of driving vehicles independently without a driver. Their 5G Remote driving service provides remote driving service during emergency situations from remote human operators [3]. These vehicles are used to provide “robotaxi” services in Beijing, Changsha, and Changzhou [3]. One of the primary use cases for the connected vehicles is safety, via rapid vehicle-to-everything communications [4]. Since drivers can be alerted to nearby disruptions, such as bad weather conditions, they can reduce the chances of traffic accidents by avoiding places with disruptions. It can potentially improve road safety anywhere in the world. However, there are ethical dilemmas of connected vehicles such as human rights, security, and societal benefits. For example, the vehicle’s location can be leaked or hacked, violating user rights to privacy. In this section, the ethical dilemmas of connected vehicles and their technological and societal solutions are explained in detail.

## 2.1Latency and Connection Stability of Connected Vehicles

The time taken for data to travel from a transmitter to a receiver is latency. Any delays in the data transmitted within the car can have consequences that are catastrophic. For connected cars to function effectively and safely, achieving the transmission of ultra-high-bandwidth data with near-zero latency is crucial [5]. As more sensors and applications are added, even more data must be transmitted to many receivers and compute units in the car, increasing the latency of data transmission. Additionally, the stability of the connection between connected vehicles also becomes non-negotiable. If the connection is interrupted by accident or on purpose, or there are lags in the data that the remote human operator receives, this could result in death in the context of remote driving, as the human operator may not be able to make the best decision for the vehicle in the event of an emergency. In this case, as laws and regulations regarding connected vehicles are not yet complete [6], the person who is responsible for the death is not clear. It could be the company of the vehicle, passenger, or remote human operator; hence it is not clear who is legally and morally responsible for any death caused. However, to say the passenger of remote driving is the one who is responsible for the death, due to their inattention on the traffic is a form of defamation since there was not time for them to act just in time to prevent the accident [7]. The level of vehicle automation also makes the problem more complex. Another option is to hold the manufacturer of the vehicle responsible, as they have the duty ethics to have their own set of rules and principles on ensuring the safety of vehicle users, rather than being forced by the authorities follow vehicle regulations. But to hold the vehicle manufacturers entirely responsible may not be ethical, as this would put a damper on the development of connected vehicles, and thereby result in lost societal benefits from the connected vehicles, such as better consumer experience while being in the vehicle. It is also unethical to hold the remote human operators responsible, if the accident is caused by the delay in data received. Although they are in control of the vehicle during the emergency, any delays or interruptions will severely impact the decision they make. Furthermore, there is the argument that the passengers still have a moral responsibility when there is an accident, as they knowingly took the risk to ride in a vehicle that switches to remote driving during emergencies.

## 2.2 Cyberthreats

Currently, successful cyber-attacks on connected vehicles are mostly caused by information exchange and wireless communications via the Internet [8]. As a result, information and data leakage are one of the most important security and privacy issues for autonomous vehicles. Here, we define ‘hacking’ as an intentional attempt by a user that is not granted permission to control the vehicle in any way. For vehicle manufacturers, the appeal to automated vehicles is the potential for greater passenger safety. However, the ethical dilemma is that automated vehicles themselves have the potential to be a threat when hackers that can exploit flaws in cybersecurity systems exist. Founder of Tesla, Elon Musk once mused of the possibility of hackers hacking into an entire fleet of connected vehicles and making all of them go to Rhode Island. The damage caused by such a hack might be so much that none of the insurance policy or class-action lawsuit would be able to compensate for it. Therefore, the public may not desire the improvements in the safety of transportation to be accompanied by the increase in likelihood of privacy invasion or increase in societal risk. Indeed, trading lower risk of deaths from traffic accidents for new cyber risks such as cyber surveillance is not justifiable. The potential security threats that come from the hacking of self-driving vehicles oppose Article 3 of the Universal Declaration of Human Rights [9], which states that “Everyone has the right to life, liberty and security of person.” For vehicle manufacturers, they have the moral duty to make the design of vehicle testing and validation of the vehicles transparent to the public to ensure greater societal understanding of the self-driving features, as well as to gain the trust of the public that the risks of connected vehicles are lower than conventional vehicles.

## 2.3 Solution

The use of 5G can potentially reduce latency. The difference between latency of 4G compared to 5G is 20 milliseconds to the 1-5 milliseconds of the 5G network [10]. As human reaction speed is about 200 milliseconds [10], traffic accidents can happen when the driver is unable to react in time to sudden changes to the road conditions. 5G’s reliable communication and low latency enhances driver-assistance systems so that drivers can react in time given the time sensitive information [10], such as the presence of animals nearby crossing the street and speeding vehicles. Consequently, drivers can avoid accidents, and remote human operators can make better decisions during remote driving mode without delay in data received.

As vehicles move enter and exit networks rapidly, that means there is the need for real-time updates and information exchange between road-side-unit and vehicles. Hackers can introduce a malicious node that adds a time slot to cause unwanted delay in the exchanging of information [8]. This is known as timing attacks which can lead to accidents happening especially in vehicles with remote driving or autonomous vehicles, where a delay in information exchanges can result in traffic accidents. Existing solution for timing attacks on connected vehicles is to force all vehicles to have fixed data rates for receiving and transferring data [8].

To prevent interruptions in the connection due to hacking or cyberattacks, Baidu has launched an automotive cybersecurity lab in China that research vehicle cybersecurity technologies, trends as well as innovations in connective vehicles [11]. The lab focuses on the best security practices in data protection, and countermeasures to fake signals used by hackers to misguide the vehicles [11]. This helps to prevent hackers from successfully attacking the connected vehicles, by constantly upgrading and updating the technology used. By keeping the connective system updated, hackers have less chance to hack successfully as they are always one step behind the updates. Vehicle owners also have the responsibility to keep their vehicles updated when there is an important security update, which the manufacturers can also monitor and share the responsibility. An example of a connected vehicle getting hacked is the ‘Uconnect’ system that uses the cellular network to let owners use smartphones to control their vehicle to start the engine remotely and gain information on the location of the vehicle. As a result, in 2015 1.4 million vehicles were recalled as cyberattacks on the system allowed hackers to remotely control a jeep’s digital system that is connected to the Internet [8]. The recalled vehicles had its software updated to prevent hacking. If a vehicle has been successfully cyberattacked or hacked, there must be a warning system in the vehicle to immediately inform both the owner and the manufacturer, so that the owner can be informed to not use the vehicle in case of malicious actions from the hacker. Owners have the moral duty to not intentionally cause harm to others, and by knowingly using the hacked vehicle despite the warning, they are violating the moral duty. The warning system will minimize the damage that a breached vehicle can cause by preventing the owner from using the hacked vehicle. Additionally, the vehicle manufacturer has the moral duty to ensure the safety of the vehicle owners. By recalling and fixing the vehicle, owners can be at ease that their vehicles will no longer be hacked.

While passengers may not have the moral duty to prevent accidents in the case of self-driving or remote driving [12], and vehicle manufacturers should not be entirely responsible for accidents due to remote or autonomous driving. Therefore, sharing the cost of accidents among all vehicle owners as well as vehicle manufacturers through mandatory insurance could be a potential solution for the ethical dilemma [12]. This system would divide the liability between owners and manufacturers, as the owners will pay for parts of the costs of accidents and the manufacturers are liable for the remaining of the costs. This way, vehicle manufacturers could still be incentivised to innovate and create better vehicles, while owners would also be incentivised to remain alert of the traffic conditions, and request for help in time in the event of emergencies or take back control when the situation calls for it. An example of legislation for self-driving vehicles is the insurance rules introduced by the Vehicle Technology and Aviation bill in the United Kingdom [13].The VTA Bill included automated vehicles to be under the compulsory motor insurance requirement. Insurers are liable for costs due to accidents caused by vehicles in self-driving mode, however they are not liable if the accident was due to the person in-charge’s carelessness, to continue self-driving mode when the situation is inappropriate. For example, there are signs of malfunction or delay in remote driving or self-driving mode that the person in-charge could have noticed. Insurers also have the right to request from the vehicle manufacturer to pay a portion of the pay-out [14].

# 3. Home Security

The rapid development in IoT and home technologies saw the proliferation of home security technologies, from motion sensors to remote cameras. Smart alarm systems installed in homes provide 24/7 home security by sending a signal to the appropriate authorities or the user’s smartphone whenever it detects an intrusion of the property [15]. Some of these include a surveillance camera that is accessible from the user’s smartphone and grants the user visual information of the entire house [16] [17]. Wireless doorbell cameras also allow home users to visually check the identity of a visitor without the need of being there physically, reducing the possibility of home robberies [17].

The actual benefit of home security technologies are not the capabilities they provide to home users to subdue malicious intruders directly, but instead, it is the deterrence they provide towards them. A UNC Charlotte study in 2018 interviewed randomly selected jailed inmates in North Carolina, Kentucky and Ohio and found that about 60% of them revealed that the presence of an alarm system would deter them from breaking into the house [18]. The benefits of home security technologies go beyond providing deterrence for the specific home. Collectively, they provide deterrence for the neighbourhood against malicious behaviours. A study conducted by Rutgers University in collaboration with the Newark Police Department attributed the drop in burglaries and the city’s crime rate to the installation of home alarm systems [19]. While many studies recognised the deterrence effect of home security systems, this is the first study to conclude the ability of home security systems to deter burglaries without displacing them to other targets [19]. The 2-year study was able to isolate other factors that affected the crime rate and observe the improvement in crime rate due to the home security systems by studying 5 years of police data [19].

## 3.1 Ethical Dilemmas

However, such powerful and connected monitoring systems inevitably introduced many controversies about its societal impacts and uses. For one, such technologies can be exploited by companies to monitor their consumers and invade their privacy. Ring, a home security systems firm owned by Amazon that sells doorbell cameras was found to have partnered with more than 400 police forces around the United States that allow them access to users’ recorded footage [20]. Ring has a social media application called “Neighbours” where users share security concerns within 5 miles of the location [20]. As big companies such as Amazon are known for data collection of their consumers, this discovery sparked controversy considering that Ring is owned by Amazon, which means that users’ data collected from these security devices could have been exploited by the company for monetary gains as in the case of the partnership with the police. This evidently violated rights ethics as each individual should hold their own control and rights in allowing access to their own data and information, instead of the companies behind these technologies. Besides, the “Neighbours” application automatically registers users into the programme as soon as the device is installed, which violates the rights of users to decide whether to be registered for it. Furthermore, the partnerships with police for monetary gains violated virtue and duty ethics. The virtue that was violated is honesty as the partnership with the police was not disclosed to the consumers. Additionally, when consumers bought the product, the firm have a duty in protecting the footage and respecting the consumers’ privacy, but instead, they sold the footage to the police without their consent.

Companies might not be the only ones to abuse home security technologies. Ironically, many home security systems were found to contain security flaws that hackers can exploit to gain access to these security systems. In 2020, an article published by The Straits Times revealed that home security cameras in Singapore were hacked and the footage were uploaded onto pornographic sites [21]. These footage revealed revealing and explicit scenes of the victims where their faces can be clearly identified in the video clips. One of the victims included a teenage girl who could be seen in revealing clothing alongside her schoolbooks. The footage was found to belong to a group dedicated to hacking Internet Protocol (IP) cameras and claimed to have access to more than 50,000 hacked cameras. In a separate incident published by Bloomberg in March, a group of hackers claimed to have gained access to live feeds from 150 000 surveillance cameras inside police departments, schools, prison and more [22]. Since some of these cameras utilised facial recognition algorithms, the hackers have access to the victims’ identity and information. From the perspective of the firm behind these technologies, duty ethics were violated as it is the firm’s responsibility in ensuring that the technologies they produced were as secure as possible. From the perspective of the hackers, rule utilitarianism and right ethics were violated. The hackers have violated the rule of invading people’s privacy and other people’s privacy rights.

In certain situations, home security technology has been turned into a modern weapon of privacy intrusion. Hidden cameras are placed in homes or companies as a form of security systems, but when they are installed with other malicious intents instead of security itself, ethical concerns arise especially if visitors are not aware and consensual of them. Hidden cameras are often installed in Airbnbs and hotel rooms and modern connective technology allows the culprit to control the device and collect data and information of visitors without their knowledge or consent [23]. According to an article published on 30th March by the Global Times, an undercover investigation revealed numerous unsuspecting shots of homes and venues, including a video of a couple living their lives in a hotel room [24]. In the video, their conversations can be clearly heard as well. This evidently violated rights ethics as this once again breached the victims’ privacy rights. Furthermore, virtue ethics in terms of honesty is violated as the victims were unaware (and thus, non-consensual) of the filming.

The line between ethical and ethicality becomes difficult to distinguish when situations where the placement of home security systems intrudes the privacy of another party unintentionally. Modern technology has improved the performance of home security systems where the area of data collection sometimes spans so large that it invades neighbouring parties’ private space, possibly causing arguments and bad blood between neighbours. In these situations, even though virtue ethics is satisfied from the point of view of the user as the user was not aware of such intrusion and have no intentio n of violating other people’s private space, duty ethics is not satisfied as users should have a responsibility in ensuring a better placement angle or location of the technology.

## 3.2 Solution

Current solutions are already in place to address these ethical issues surrounding privacy concerns. For example, the Personal Protection Data Act (PDPA) is a Singapore law that serves to protect personal data [25]. According to the Personal Data Protection Commission (PDPC), offences include accessing personal data without the individual consent and may be subjected to various forms of penalties [25]. For example, on 14 October, ChampionTutor was imposed upon a $10 000 fine for causing the leaking of personal data by failing to impose appropriate security measures [26]. Such enforcement might deter firms from abusing consumers’ data and might even encourage them from reinforcing security measures.

However, rules and regulations alone are insufficient as they cannot cover the entirety of personal data abusers and exploiters. Hence, technological solutions should be implemented to prevent entities such as hackers that are able to get around or have no regard for rules and regulations. Besides reinforcing security measures, these home security technologies can be installed with options to turn on or off the sending of information to the central monitoring station or even to delete stored personal data. With these options, users can choose when they do not want to take the risk of privacy breach especially in vulnerable situations such as typing in credentials on a home computer or changing of clothing in bedrooms. In the example of Ring as mentioned earlier, users should be given a choice whether to be enrolled into the “Neighbours” programme and thus, these would satisfy rights ethics as the users would now have the option to exercise their rights of privacy control.

Moreover, technologies are not fail-safe and solutions to these ethical dilemmas should ultimately depend on individual responsibilities. A possible solution would be for the companies involved in the home security technologies to ensure the devices as well as the data stored are as secured as possible. Additionally, they should exercise the consumer’s privacy rights by requesting for consent whenever there is a need to access the user’s data, as well as ensuring that the consumers are well informed of their data usage and handling details. This process is modelled as an ethics decision flow chart from the perspective of the firms shown in the following figure:

Diagram

Description automatically generated

Figure 1: Ethics Decision Flow Chart

Other than the firms, society plays a role in solving such ethical dilemmas as well. Societal roles include the rejection of unwanted and malicious behaviours such as hacking. Although there is a consensus that hacking is unethical due to rule utilitarianism being violated and the freedom and privacy rights of people are breached, due to monetary gains, hacktivists are able to justify such actions as the rewards, be it monetary or personal utility, exceeds the costs and risks. Hence, societal rejection of such behaviours can be emphasised through the introduction of harsher punishment. Such punishment should not only be administered to the hacktivists, but to any parties in the involvement of violating data privacy so as to undermine the rewards obtainable from such behaviours. Yet, punishment have to be carefully balanced in order not to inflict a punishment far greater than the intrinsic cost of the unwanted actions as the purpose of punishment is to deter such behaviours instead of just removing “utility” from the wrongdoer. In the event of a security breach, victims should also be compensated adequately by the responsible parties which include the culprit and possibly the firm if the firm’s negligence is found to have contributed to the security breach.

Consumers’ responsibilities in solving the mentioned ethical dilemmas include ensuring security of personal data on their end. Fundamental security of personal data such as using of a secure password or simply not spreading of one’s password should be enforced and hence, satisfying duty ethics. According to a report by Verizon in 2019 on data breaches, weak passwords contributed to 80% of data breaches due to hacking [27]. As more powerful technological tools emerge, practicing good security habits become increasingly more important as consumers have to cooperate with firms in ensuring the safe and secured use of such technology; as firms release security updates of devices, consumers also have to play their part in constantly checking for these updates and installing them. If a user practices poor security habits, it is unjust for the firms behind the technologies to shoulder the entire blame of “weak security” when a breach occurs as the negligence of the user could equally have contributed to the breach as well.

## 3.3 Consequences on Future Generations

Peace and security are instrumental to societal development and individual well-being and is an aspect that can benefit much from the advancement of technology. With the better responsiveness and connectivity of home security technology and identification system, victims and relevant authorities can react faster and more empowered to prevent malicious acts from happening. Furthermore, the deterrence they provide can subdue malicious demeanours and keep overall crime rate lower. For future generations, this could mean a better peace of mind and greater quality of life.

However, technological advancement empowers individuals of future generations with greater access to more powerful tools that can cripple data security. Hence, there is a need for firms and consumers in the future generation to upkeep their security measures and constantly find and fix security flaws. Nevertheless, many of the ethical dilemmas can be resolved by changing individuals' and societal behaviours and mindset.

# 4. Health Trackers

Health trackers, or wearable activity trackers are electronic devices that enable users to track and monitor their health status through several metrics [28]. The number of steps throughout the day and week, sleeping times and patterns, and eating habits is the usual metrics used by wearable activity and health trackers to track a person’s health. Simpler devices just display the recorded data for the user’s own judgment, whereas more advanced health tracking systems are able to track the user’s data over a long period of time and produce several insights and tips for users to improve their life habits. This shows that these devices are heavily dependent on users’ data to general useful insights and improve users’ judgment.

The dependency of health trackers on users’ health data, which could be argued is considered private, also means that the companies that sell these devices also must be responsible to store the users’ data, which brings up the ethical dilemma regarding the storing of users’ private data by external companies. This data could give access to some private information about the user, such as the times when the user is outside their home, or information regarding the organization and/or company that the user works in [29].Moreover, the security of these devices is concerning as research from Goyal, Dragoni, and Spognardi shows that even the most commonly used health trackers are vulnerable to cyber-attacks [30]. Hence, the users’ data is also at risk to be accessed by external parties outside of the companies that are handling the data. Thus, in this section, we will look deeper into the ethical dilemmas of health trackers by dividing them through various parameters such as human rights, security, and societal benefits. We will analyze each case using several ethical theories and using the ethical line diagram with possible scenarios. Lastly, recommendations would be made to give insight into what action would be the most ethical for both the users and companies.

## 4.1 Storage and Handling of User’s Health Data

Companies that market and make use of wearable health trackers and/or activity trackers need to have access to the users’ personal data to track several metrics such as the number of steps, sleeping times, and eating habits. Some of the user’s personal data such as the users’ location, would be used to calculate several metrics such as the number of steps and distance travelled by the user throughout the day. Another example would be storing users’ eating habits and foods to track the calories consumed throughout the day. From the users’ personal data, the companies could employ sophisticated algorithms and implement clever technologies to calculate necessary metrics and give valuable insights to their users on how to improve the health status of users. Thus, it is inevitable that in order for trackers to work, companies need access to the users’ data, and the companies’ handling of such data would be the main ethical dilemma that we want to focus on.

Ethical dilemmas regarding the storage and handling of users’ data by the respective companies would not be solved solely by looking through the perspective of human rights. Based on a paper published by Harris and Wyndham [31], human rights would not solve all ethical questions regarding the sharing of data of an individual, but it gives rise to new questions for consideration, in particular the corresponding parties involved in the ethical issue. Looking from the lens of human rights gives us the chance to look at the connection between the policies and practices of data sharing with the individuals involved and the socio-political situation surrounding the matter [31]. Hence, if we are analyzing the ethical dilemma regarding data storage and sharing actions using human rights, we should consider the policies and regulations to control data sharing and the companies’ role in storing the data. Thus, for subsequent analysis based on ethical theories, we will be looking from the perspective of the users and the companies’ perspectives. Furthermore, to set a standard for the regulations that apply for controlling data protection, we will set Singapore’s data protection law, which is the Personal Data Protection Act (PDPA) as the standard [32].

## 4.2 Ethical Dilemmas Regarding Health Data Privacy

For the ethical dilemmas, we will be using some of the ethical theories that have been taught in class, mainly utilitarianism and rights ethics. The reason is that utilitarianism gives us an understanding of whether the scenarios would benefit each party, and society, that is involved. In addition, rights ethics would be the second ethical theory that we will use, as ethical problems regarding human data privacy will be closely related to fundamental human rights such as rights to privacy. We will be referring to human rights laws mentioned in the Universal Declaration of Human Rights (UDHR) for our arguments and baseline. Based on these two ethical theories, we will then put scenarios into an ethical line diagram to compare which scenarios would be relatively worse in terms of ethics and provide solutions and suggestions from there.

Before moving into the ethical theory analysis, we need to set the ideal scenarios and possible real-world scenarios regarding the handling of users’ health tracking data. We shall label an ideal situation as Positive Paradigm (PP). An ideal ethical situation regarding the storage of user’s health data is when the user has given consent to the company, based on the document “Guide to Data Sharing” from the Personal Data Protection Commission (PDPC) in Singapore [33]. Furthermore, the data stored would only be used by the company to calculate health metrics and provide insights to the corresponding user. If the company needs to cooperate with other companies or data intermediaries to provide such insights, such as location tracking services, then there should be written contracts between the company providing health tracker and the data intermediary to indicate that the user’s personal data shall not be used by the data intermediary for other purposes [33], in this case, other than for health tracking purposes. Additionally, users should ideally be given control and freedom to read, update, and delete their personal health data. This is done because their personal data is considered to be their privacy, which is a fundamental human right according to many international human rights organizations [34].

On the other side of the spectrum, we would have unethical handling of users’ health-tracker data, which is basically the opposite case from the ideal situation. We shall label this scenario as a Negative Paradigm (NP). In this scenario, the user’s steps, location, sleeping, and meal data would be taken without consent by health-tracking companies without any contracts and there are no limitations regarding sharing of user’s information to external parties. In addition, users have limited control over the health and location data that they have in their health tracking devices and the companies would exploit the user’s data for further decision making and policymaking to their benefit.

In between, we have found some real-world cases that we could extract for the ethical line analysis, which we would label Point 1 (P1) and Point 2 (P2). P1 would refer to similar cases such as a case study from a BBC article titled “The Rise of Employee Health Tracking” [35]. In this case, employees’ health would be monitored using patches attached to the employees’ body and the data would be transmitted to the employees and their company to monitor their employees’ health status. Although this is an innovative way to monitor the health of employees, especially taking into consideration the COVID-19 situation, it could also be argued that this move poses some risk regarding the intrusion of the employees’ privacy and the companies would use the employees’ data for unethical decision making. In the article, it is mentioned that companies that have access to their employees’ health data could employ some unethical policies and decisions such as denying promotions to less-fit employees [35]. Thus, we could generalize P1 to similar cases where a company would have consent from their users and/or employees to store their health data and they would have written contracts with some external parties regarding the handling of personal data, but the company would also use their data for their gains as well through their policies and management decisions.

On the other hand, P2 would refer to similar cases to real-world cases where users’ data would be sold and/or given to third parties. A paper by Challa, Yu, and Kunchakarra that discusses the exploitation of wearable health technology showed that users’ data from health and fitness apps are transmitted to various third parties, including advertisers [36]. This means that the user’s data was transmitted to external third parties for other purposes, such as selective advertising to the users. The paper even mentioned that some of the data transmitted to external parties included names and addresses of users [36]. Thus, we could generalize P2 to similar events where a health-tracker user has given consent for his/her health data to be taken, but the health data would be sent to miscellaneous external parties for purposes other than tracking the user’s health metrics and giving users insights.

In addition, we could also consider one possible scenario regarding the storage and handling of users’ health data, which we could label as Possible Scenario 1 (SC1). A possible scenario that was not mentioned in both P1 and P2 is the instance when the user has given consent to store their data, but the company also gathers some additional data, metadata, or other information related to the user’s health data. For example, users’ location data from Google could also contain the particular time of day when they are outside their homes, visit certain places, etc. Companies could take advantage of these data and metadata for their purpose, similar to the case in P1. Companies could also sell these metadata to external parties, which is similar to the case in P2. Hence, gathering users’ data with consent and analyzing its metadata for the companies’ purpose or external parties’ purpose would be a serious possible issue that we would like to analyze.

From the perspective of the companies, utilitarianism is satisfied in all scenarios PP, NP, P1, P2, and SC1. In all these cases, the companies would create wearable health devices that could track users' health and give insights, which would benefit society as a whole. In a sense, this data could also be beneficial for the companies as they might know the flaws and drawbacks of their system and take corrective actions. Particular attention should be given to cases NP, P1, and SC1. In these three cases, the health data of users would be used not only for the benefit of the society but also for the benefit of the company themselves as they could produce regulations based on those data to benefit specifically themselves. An example of such a policy could be seen in the BBC article regarding health tracking of employees, which is denying promotion of employees who are deemed less fit/healthy, based on their health data collected [35].

From the perspective of the users, utilitarianism is also satisfied in all scenarios PP, NP, P1, P2, and SC1. The data gathered from the devices would be used for the user’s benefit to track their own health conditions and provide insights on their daily activities, such as the number of calories that should be eaten, sleep times, etc. Furthermore, gathering health data of users would be beneficial for future technological developments such as connecting users’ health data to hospitals, which could help to streamline the process of booking appointments. However, before getting into future implications, we should look at the potential misuse of user-health data. In this case, data gathered by the companies could also be used for other malicious purposes, which might not be for the greater good of the users. As mentioned in the previous paragraph, cases NP, P1, and SC1 are at most concern, as companies and external parties could take action that would benefit themselves and put the users at a disadvantage, as showcased in the previous paragraph. Overall, we could say that utilitarianism is satisfied for the users as long as the health-tracking system works for their benefit.

Next, we will investigate the rights ethics from the perspective of the companies. For cases PP, rights ethics will be satisfied as the user’s health data would be used accordingly for health tracking purposes and not for any malicious attempts. However, for cases NP, P1, P2, and SC1, rights ethics would not be satisfied as users' data would not be protected from misuse by companies and/or external parties, which is a violation of the purpose of PDPA [32]. This would also violate the United Nations Universal Declaration of Human Rights (UDHR) Article 12, which states that “No one shall be subjected to arbitrary interference with his privacy” [9]. Thus, we could conclude that for the majority of cases except for PP, rights ethics would not be satisfied. We shall look into each case in particular.

Looking into detail, we could see that NP has the worst privacy violation, as the user’s data is taken without consent and their data is misused by the company and shared with external parties. Continuing, we could argue that P2 is a worse violation of data privacy compared to P1, as users’ data is shared with more and more malicious parties, thus having a greater chance of data misuse by external parties. Meanwhile, in P1’s case, data privacy violation was done only by the company in question. On the contrary, we would also argue P3 would have worse privacy violations, as events from P1 and P2 might happen in P3. However, we still consider P3 is the ethically better case compared to NP as the company still asks for consent for the users’ data.

From the perspective of the users, they would satisfy rights ethics for all the cases PP, NP, P1, P2, and SC1. In all these scenarios, users have the right to own their own property, in this case, health tracking devices, for their own purposes. This is in accordance with UDHR Article 17 which states that “Everyone has the right to own property alone as well as in association with others” [11]. They also have the right to give or not to give consent to the companies to give access to their data. Thus, in a sense, users have the initial control to give their data to the companies. Overall, we could say that rights ethics is satisfied for the users.

Based on the ethical theory analysis using utilitarianism and rights ethics above, we could create an ethics line diagram. We will create the ethics line diagram based on the perspective of the companies. The following diagram represents the ethics line diagram of cases PP, NP, P1, P2, and SC1:



Figure 2: Ethical Line Diagram Analysis

|  |  |  |
| --- | --- | --- |
| Scenario | Ethics Line Drawing | Location |
| PP | Asking for users’ consent, health data used just for health-tracking purposes, valid written documents for health and location data sharing to external parties, users’ have full control over their health data. | Right Point |
| NP | No user consent, data collected also used by companies for their own benefit, selling or sharing of users’ personal data to external parties, users’ have limited control over their data. | Left Point |
| P1 | Asking for users’ consent, but users’ health data is also used by the company for their personal gains. | Approx. 6.5/10 |
| P2 | Users’ health data would be sold and/or given to external parties and the data would be used for other purposes. | Approx. 4.5/10 |
| SC1 | Users would give consent, but users’ health data and metadata would be used by the companies and also would be shared with external parties unnoticed. | Approx. 2/10 |

Table 1: Description of the Ethical Line Diagram

The ethical diagram above was made based on our previous ethical theory analysis. It could be seen that P1 has a relatively higher standing than P2. This is in accordance with the analysis based on rights ethics, as in the case of P2, data could be misused by more than one party. It also could be seen that SC1 is lower than P1 and P2, which is also in accordance with the rights ethics analysis. This is because, in SC1, events in P1 and P2 might happen, which should make it in a worse ethical standing compared to P1 and P2.

## 4.3 Solution

The solution to the data storage privacy problem lies in the data protection laws of each country. In Singapore, we have the data protection rules, which is PDPA, and each health-tracking company should abide by the rules set by PDPA. However, research by Vitak et al. regarding the attitudes of fitness tracker users towards privacy and data valuation found out that some of the data privacy rules and/or policies set by some health-tracker app creators such as Fitbit and Jawbone could be ambiguous [37]. Some of these companies set their data privacy rules in such a way there could be gaps where they could extract extra information and/or share the information with other parties. In the research’s case, Fitbit and Jawbone didn’t make it clear whether the information that they would not share encompasses the data that the fitness trackers generate [37]. Thus, we could deduce that data privacy laws alone could not stop all cases of data privacy violations.

Another solution would be for the users to be more mindful regarding the data consent that they are giving to health-tracker companies. Although this seems to be a generic solution, research by Vitak et al. proved otherwise. Their research showed that there exists a privacy paradox, where there is a sense of cynicism and apathy regarding online privacy [37].They also mentioned that privacy-protective behaviors would lead users to believe that data would eventually be shared, which leads to an understanding of the inevitability of privacy violations [12]. Thus, users should also be mindful that, although health-tracking devices could be useful to monitor their health, they should also be wary regarding the data they have consented to give through the health-tracking devices.

# References

|  |  |
| --- | --- |
| [1] | [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8972389. |
| [2] | K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, “Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends, and Prospects for Emerging 5G-IoT Scenarios,” IEEE, 2020. |
| [3] | Baidu, 16 December 2020. [Online]. Available: https://www.technologyreview.com/2020/12/16/1014672/building-a-self-driving-car-that-people-can-trust/. [Accessed 22 10 2021]. |
| [4] | J. Locke, “What Is Connected Vehicle Technology and What Are the Use Cases?,” 17 June 2020. [Online]. Available: https://www.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases. [Accessed 16 October 2021]. |
| [5] | D. Schwartzberg, 31 October 2019. [Online]. Available: https://www.electronicdesign.com/markets/automotive/article/21808774/invehicle-data-latency-fast-or-furious. [Accessed 20 October 2021]. |
| [6] | Z. G. ,. Z. W. Xi Zhu, “Ethical Challenges and Countermeasures of Autonomous Vehicles,” p. 5, 2021. |
| [7] | A. H. &. J. Nida-Rümelin, “Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis,” p. 12, 2014. |
| [8] | X. Z. K. J. R. A. S. L. Y. Z. Y. X. S. Y. Mahdi Dibaei, “Attacks and defences on intelligent connected vehicles: a survey,” p. 23, 2020. |
| [9] | U. Nations, “Universal Declaration of Human Rights,” 1948. |
| [10] | Ericsson, 2021. [Online]. Available: https://www.ericsson.com/en/5g/5-things-to-know-about-5g-if-you-work-in-the-auto-industry. |
| [11] | Baidu, 16 December 2020. [Online]. Available: https://www.technologyreview.com/2020/12/16/1014672/building-a-self-driving-car-that-people-can-trust/. [Accessed 22 October 2021]. |
| [12] | T. Ampe, 12 December 2020. [Online]. Available: https://vce.usc.edu/volume-4-issue-2/autonomous-accidents-the-ethics-of-self-driving-car-crashes/. [Accessed 19 October 2021]. |
| [13] | “GOV.UK,” 22 February 2017. [Online]. Available: https://www.gov.uk/government/news/new-measures-set-out-autonomous-vehicle-insurance-and-electric-car-infrastructure. [Accessed 20 October 2021]. |
| [14] | A. Z. Mark Schaub, 29 August 2017. [Online]. Available: https://www.kwm.com/en/knowledge/insights/self-driving-cars-who-will-be-liable-20170829#id-here. [Accessed 20 October 2021]. |
| [15] | Ackerman Security, “Local vs Central Alarm Systems: What’s the Difference?,” [Online]. Available: Local vs Central Alarm Systems: What’s the Difference?. [Accessed 26 October 2021]. |
| [16] | Home Stratosphere, “Complete Wireless Doorbell Guide: Options, Pros and Cons,” Home Stratosphere, [Online]. Available: https://www.homestratosphere.com/wireless-doorbells/. [Accessed 26 October 2021]. |
| [17] | Bastion Security, “Video Surveillance,” Bastion Security, [Online]. Available: https://www.videosurveillance.com/tech/mobile-and-remote-camera-systems.asp. [Accessed 26 October 2021]. |
| [18] | J. B. Kuhns, “Understanding Decisions to Burglarize from the Offender's Perspective,” Research Gate, North Carolina, 2012. |
| [19] | Rutgers University, “Rutgers Study Finds Alarm Systems Are Valuable Crime Fighting Tool,” Rutgers University, 5 February 2009. [Online]. Available: https://www.rutgers.edu/news/rutgers-study-finds-alarm-systems-are-valuable-crime-fighting-tool. [Accessed 26 October 2021]. |
| [20] | R. Molla, “How Amazon’s Ring is creating a surveillance network with video doorbells,” Vox, 28 January 2020. [Online]. Available: https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks. [Accessed 26 October 2021]. |
| [21] | The Straits Times, “Singapore home cams hacked and stolen footage sold on pornographic sites,” The Straits Times, 12 October 2020. [Online]. Available: https://www.straitstimes.com/singapore/singapore-home-cams-hacked-and-stolen-footage-sold-on-pornographic-sites. [Accessed 26 October 2021]. |
| [22] | W. Turton, “Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals,” Bloomberg, 10 March 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. [Accessed 26 October 2021]. |
| [23] | S. Fussell, “Airbnb Has a Hidden-Camera Problem,” The Atlantic, 27 March 2019. [Online]. Available: https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/. [Accessed 26 October 2021]. |
| [24] | Global Times, “Media investigation exposes thousands of candid shots shared and sold via social media platforms,” Global Times, 30 March 2021. [Online]. Available: https://www.globaltimes.cn/page/202103/1219872.shtml. [Accessed 26 October 2021]. |
| [25] | Personal Data Protection Commission, “Personal Data Protection Commission,” PDPC, [Online]. Available: https://www.pdpc.gov.sg/. [Accessed 26 October 2021]. |
| [26] | PDPC, “Breach of the Protection Obligation by ChampionTutor,” PDPC, 14 October 2021. [Online]. Available: https://www.pdpc.gov.sg/all-commissions-decisions/2021/10/breach-of-the-protection-obligation-by-championtutor. [Accessed 26 October 2021]. |
| [27] | K. Bowen, “Are Pwned Passwords Putting Your Business at Risk?,” InfoSecurity Magazine, 16 October 2019. [Online]. Available: https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/. [Accessed 26 October 2021]. |
| [28] | G. Shin, M. H. Jarrahi, Y. Fei, A. Karami, N. Gafinowitz, A. Byun and X. Lu, “Wearable Activity Trackers, Accuracy, Adoption, Acceptance and Health Impact: A Systematic Literature Review,” Journal of Biomedical Informatics, 2019. |
| [29] | M. Rahman, B. Carbunar and U. Topkara, “Secure Management of Low Power Fitness Trackers,” 2017. |
| [30] | R. Goyal, N. Dragoni and A. Spognardi, “Mind the Health Tracker You Wear - A Security Analysis of Wearable Health Trackers,” 2016. |
| [31] | T. L. Harris and J. M. Wyndham, “Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing,” *Journal of Empirical Research on Human Research Ethics,* vol. 10, pp. 334-337, 2015. |
| [32] | “PDPA Overview,” Singapore Government Agency Website, [Online]. Available: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. [Accessed 23 10 2021]. |
| [33] | P. D. P. Commission, *Guide to Data Sharing,* Singapore, 2018. |
| [34] | Privacy International, “The Right to Privacy in Singapore,” 2015. |
| [35] | D. Cox, “The Rise of Employee Health Tracking,” BBC, 11 11 2020. [Online]. Available: https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking. [Accessed 23 10 2021]. |
| [36] | N. Challa, S. Yu and S. Kunchakarra, “Wary about Wearables: Potential for the Exploitation of Wearable Health Technology Through Employee Discrimination and Sales to Third Parties,” Intersect, 2017. |
| [37] | J. Vitak, Y. Liao, P. Kumar, M. Zimmer and K. Kritikos, “Privacy Attitudes and Data Valuation Among Fitness Tracker Users,” Springer International, 2018. |
| [38] | [Online]. Available: https://www.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases. |
| [39] | J. Locke, “What Is Connected Vehicle Technology and What Are the Use Cases?,” 17 June 2020. [Online]. Available: https://www.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases. [Accessed 19 October 2021]. |
| [40] | United Nations, “Universal Declaration of Human Rights,” in *United Nations*. |

**Honour Pledge**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Year*** | ***Semester*** | ***Project Title*** | ***Tutor*** |
| **2021-2022** | **1** | **Next-Generation Connected Systems** | **Prof Mansoor Bin Abdul Jalil** |

|  |
| --- |
|  |

**We, the following students of NUS, upon our honour, hereby confirm that we have neither received nor given any unauthorized help on the EG2401A group project carried out by us.**

**The project report and the presentation reflect truly our own efforts. In all cases where material from other sources such as books, articles, notes and websites have been used, we have taken care to provide clear and unambiguous references to the same.**

**We confirm that we have not provided unauthorized help to other groups doing the same project. Furthermore, we also confirm that we will not pass on our research materials, report and presentation materials to other students who may take this module in later semesters.**

**In addition, this project report has been prepared and submitted by us only as a part of an academic exercise. Its contents are not meant for publication in any manner.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Sl.No.*** | ***Matric No.*** | ***Name*** | ***Signature*** | ***Date*** |
| **1.** | A0200704Y | Gede Arya Chandradhana | Gede Arya | **27/10/2021** |
| **2.** | A0199806L | Goh Kheng Xi, Jevan | Jevan Goh | **27/10/2021** |
| **3.** | A0204751M | Lock Mei Lin | Mei Lin | **27/10/2021** |