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 a 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. 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. 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.

The actual benefit home security technologies bring 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.

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. 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. 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.

**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. Ring has a social media application called “Neighbours” where share security concerns within 5 miles of the location. [https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks]. 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 violated the rights of users to decide regarding 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. These footages revealed obscene 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 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. 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 secured 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 arises especially when 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 [https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/]. 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 about their lives in a hotel room. In the video, their conversations can be clearly heard as well. [https://www.globaltimes.cn/page/202103/1219872.shtml] 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 situation where the placement of home security system 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 this situations, even though virtue ethics is satisfied from the point of the user as the user was not aware of such intrusion and have no intention 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.

**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. 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. 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. 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 is 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 figure below.

Start: Firm selling home security products to consumer

Does anyone have access to the data/device without the user’s knowledge or consent?

yes

Duty, rights and virtue ethics violated

No

Does the user have control over personal data such as options to turn off and on data collection services?

No

Rights ethics violated

yes

Are there security flaws that allows illegal access to the data or device and are there security measures that can be reinforced?

No

Duty ethics violated

yes

Redesign the terms and conditions prior to selling the product to include the information of data handling and request consent for third party’s access if required. Additionally fix all the security bugs and strengthen security as much as possible.

Other than the firms, society play a role in solving such ethical dilemma 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.

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. [https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/]. 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.

**Consequences on future generation**

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 generation 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 individual’s and societal behaviours and mindset.

As more powerful technological tools emerge, individuals of future generation have more responsibility to play in practicing good security habits. Firms and consumer have to corporate in ensuring the safe and secured use of such technology; as firms releases security updates of devices, consumers also have to play their part in constantly checking for these updates and install them.