I'm in the development of a food delivery system using drones for the Informatics Large Practical. This service is currently provided only in the central campus area and by ordering online, drones will head to nearby participating restaurants to collect the ordered items, then deliver the order to the client. My task is to develop the basic framework of the system and an algorithm to find the best possible flight path for the drones. Since drones are a relatively recent technology being used in delivery services and the ordering system is online, there are unrealized and unintentional harm to different stakeholders that can be caused by this delivery system. This essay aims to identify and reflect on these issues.

The first glaring issue is privacy, as drones have cameras equipped and although their intended purpose is to scan surroundings and ensure safe flights, the recorded data will be uploaded to the system's database, hence the geolocation or visual data collection will happen unavoidably on individuals who didn't specifically consent to such actions. This unintentional harm can cause severe consequences as not only personal information are collected without consent, but if the drone is compromised and remotely controlled by an unauthorized user, it could be used for malicious purposes such as tracking, doxing, and surveillance. Hence, although the project is still a framework and specific drone flight procedure isn't detailed in the specification, in future development, I should be aware of these privacy flaws and ensure that unconsented stakeholders are not affected by the treatment of drone-collected data and the flight area of the drones, such as strictly using data collected for navigation and locating, and choosing drones with technologies such as auto-redacting to prevent recording visual personal information and geofencing to prevent drones from collecting data in certain pre-defined areas.[1] However, a counter-argument to be raised is that some parties such as the Royal Aeronautical Society and the Royal Academy of Engineering have expressed that the pre-existing legislations have already addressed the privacy concerns to an extent, as under the current legislation, a drone's threat to privacy is "unlikely to be greater than those existing from smartphone cameras",[2] hence rendering some of the privacy concerns mentioned above unnecessary to some stakeholders. Considering the different points of view, when designing the software, I need to be aware of the balance between potential privacy vulnerabilities and the necessity of some additional implementations of privacy-protecting features.

Another potential issue is safety, it includes a multitude of events that could cause unintentional harm or damage to stakeholders. Since drones are relatively fragile machines and must traverse through public spaces and densely populated areas at high altitudes, events such as taking off and landing the drone, carrying hot food, and possible collisions with other objects such as wildlife, buildings, or even other drones all pose serious security risks. In the current system specification, no-fly zones have been carefully defined to reduce safety hazards, yet it is clear that there are still various potential factors that are dangerous for users, pedestrians, and other stakeholders: the drones still must fly through other areas in the city centre, constantly changing weather conditions, damage or natural wear to the drone, etc. As I will be implementing the fly path algorithm for drones, it is my responsibility to consider and attempt to address these possible liabilities. I must program the drones to be strictly kept outside of the no-fly zones, a safe distance between buildings, and in future development, areas with more pedestrians should be avoided in route planning if possible. In situations where mitigation via software isn't effective, I should ensure

that the choice of drones in future development has sufficient physical dexterity to endure potential damage to an extent and emergency landing features to minimize the risk of damaging or harming people or properties.[1]

Apart from the drone-related issues, since all user data synchronizes with the server, potential security breaches are a legitimate concern to be faced. In 2021, 45% of US companies suffered a data breach[3] and in 2022, 21% of UK companies had experienced a data breach at least once during the last year and 18% suffered a data breach every month.[4] In the current delivery system, the structure of the recorded orders on the server includes personal information such as credit card numbers, expiry dates, and CVVs of users, there may be a significant backlash if such records are leaked. Also, the data collected from the users may be subject to irresponsible use by the food delivery system in future operations such as selling users' private information or using images of users without consent for any purpose. Although security features are not in the scope of the current specification, since I'm developing a commercial service that would be run by another stakeholder, I have the responsibility to address the system security vulnerabilities as the service must comply with the local law, which states that the stored user data must have adequate information protection to ensure "appropriate security of personal data" as required by the UK Data Protection Act 2018.[5] To achieve the stated standard, I should deploy third-party security solutions or provide sufficient security protection against malicious accesses and attacks to user data stored locally on the drone and the server. I should also ensure the exact usage of user data both within this service or with any third-party organizations are as transparent as possible and stray away from deceptive design patterns to collect inappropriate data for the corresponding service such as "Privacy zuckering".[6]

In conclusion, several factors can potentially contribute to unintentional harm from different angles to the stakeholders of this service. A service with less unintentional harm will be beneficial for all stakeholders: better reputation for the business, better user experience for the customers, a safer environment for the pedestrians, etc. Future development teams and I have the responsibilities to prevent these unintentional harms and minimize the negative impacts caused by the service to the best of our abilities.

Reference:

[1] AltiGator Drone & UAV Technologies. 2022. *Drone security features*. [online] Available at: <https://altigator.com/en/features-of-our-drones/security-features/> [Accessed 18 October 2022].

[2] House of Commons Science and Technology Committee, 2019. *Commercial and recreational drone use in the UK*. the House of Commons, p.35.

[3] Driscoll, A., 2022. *30+ Data Breach Statistics and Facts: Frequency, Impact & more*. [online] Comparitech. Available at: <https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/> [Accessed 18 October 2022].

[4] Statista. 2022. *UK businesses: frequency of cyber security breaches 2022 | Statista*. [online] Available at: <https://www.statista.com/statistics/586725/frequency-of-cyber-security-breaches-experience-by-businesses-in-the-uk/> [Accessed 18 October 2022].

[5] legislation.gov.uk, 2018. *Data Protection Act 2018*. The National Archives.

[6] Brignull, H., 2022. *Privacy zuckering - a type of deceptive design*. [online] Deceptive.design. Available at: <https://www.deceptive.design/types/privacy-zuckering> [Accessed 18 October 2022].