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 and 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 is 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 and supply potential mitigating methods for them.

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 and geolocation or visual data collection on individuals who didn’t specifically consent to such actions will happen unavoidably. 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. To mitigate this unintentional harm, the data collected from the equipped cameras should strictly be used for navigation and localization purposes, the drone flights must comply with corresponding legislations, and technologies such as auto-redacting and geofencing should be used if possible (Drone security features, 2022). Another point 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”(House of Commons Science and Technology Committee, 2022), hence rendering some of the privacy concerns unnecessary.

Another potential issue is safety, this 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 birds, buildings, planes, or even other drones, all pose serious security risks. Technically, the entirety of Edinburgh city centre is classified as a “high risk” zone and a controlled traffic region due to it being a congested airline area (Drone Safety Map | Altitude Angel, 2022). From 2014 to 2018, near-misses between drones and aircraft in the UK increased from only 9 to 125 per year (McCarthy, 2022). In the current system specification, no-fly zones have been carefully defined to reduce risks, yet it is clear that there are still various potential risks: the drones still must fly through other areas in the city centre, 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 mitigate these possible risks. The drones should be strictly kept outside of the no-fly zones and a safe distance between buildings and possibly other drones’ flight paths. The drone flight height should be kept within legislated ranges to avoid potential collisions with aircraft and 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 (Drone security features, 2022).

Apart from the drone-related issues, since all user data are synchronized with the server, potential security breaches are a legitimate concern to be faced. In 2021, 45% of US companies suffered a data breach(Driscoll, 2022) 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.(UK businesses: frequency of cyber security breaches 2022 | Statista, 2022) 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 unconsented or irresponsible use by the food delivery system in future operations as user data may be used for monetary purposes or shared with malicious organizations or entities. To address this issue, in further development, the exact usage of user data both within this service or with any third-party organizations must be as transparent as possible, the service should stray away from deceptive design patterns such as “Privacy zuckering” (Brignull, 2022), and the service should supply a clear method for any user who would like to revoke the right for the service to use their information. Additionally, although security features are not mentioned in the current specification, there are legal requirements for the service to run. Both data stored locally on the drone and user data on the server must have adequate information protection to ensure “appropriate security of personal data” as required by the UK Data Protection Act 2018 (legislation.gov.uk, 2018).

In conclusion, several factors can potentially contribute to unintentional harm from different angles to the stakeholders of this service. 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:

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].

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].

Dronesafetymap.com. 2022. *Drone Safety Map | Altitude Angel*. [online] Available at: <https://dronesafetymap.com/> [Accessed 18 October 2022].

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].

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

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

McCarthy, N., 2022. *Infographic: Drones: a rising menace to UK aviation*. [online] Statista Infographics. Available at: <https://www.statista.com/chart/16490/near-misses-between-drones-and-planes-in-the-uk/> [Accessed 18 October 2022].

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].