# Original Project Aims

An increasing number of smart-home devices are being developed to provide surveillance solutions for customers. While these devices have proved successful in improving the security of people’s homes, they introduce new unprecedented privacy risks. This project aimed to investigate homomorphic encryption as a solution to privacy concerns without detracting from the security benefits. To this end, it intended to use existing homomorphic encryption libraries to implement privacy-preserving unsupervised machine learning algorithms that can extract moving objects from surveillance footage. As extensions, the project would implement a bespoke encryption algorithm, investigate further inference algorithms, and validate the security of such algorithms.

# Work Completed

Overall, the project was a success. It fulfilled all core success criteria and obtained significant results from inference algorithms and in the optimisations applied to improve performance. Furthermore, the project was extended by implementing a bespoke homomorphic encryption scheme, furthering understanding and providing opportunities for specialisation optimisations. Security of encryption schemes was considered during the preparation stage before implementation, but a formal proof was not completed due to time constraints. Similarly, extending with object recognition was dismissed to provide a more thorough investigation of moving object detection algorithms.

# Special Difficulties

The majority of the project was completed with relatively few unexpected disruptions. However, contracting COVID-19 in December resulted in the project falling several weeks behind schedule. Consequently, significant extra work had to be done to get back on track and ensure the project was completed before the deadline.