To what extent should surveillance be justified within society?

Surveillance in modern-day society is a newly developing phenomenon, which new technology and advancements online has rapidly accelerated. Not only has surveillance's definition changed, from simply the use of security cameras, but our everyday use of mobile phones and devices holds the potential for mass security and monitoring of so many aspects of life. How much of our personal data should legitimately be accessible by the government, and does the prevention of crime and maintenance of law and order justify this? Clearly outlining as a society the limits to governing authority is essential if we want to maintain personal liberty under government.

It may be argued that surveillance should be justified largely as a security measure, which maintains the regulations of law and order within society. On public land, the domain is under the possession of the government, so therefore may have cameras or other systems introduced as surveillance methods. Although, it can be said that in order for this to be done in a fully justified and legitimate manner, a governing authority should address what exactly is being recorded, stored and analysed, for the prevention of crime. Is it simply a deterrence tactic, to place cameras in public areas? Are the faces of previously convicted criminals being tracked and recorded for monitoring reasons? Or, are the identities of the wider general public, many of whom will never commit a crime in their lives, being stored and shared silently? Not only should transparency in clarifying the uses of surveillance in this way be at the forefront of the operation, if the purpose is defined as being to reduce crime, but also the education of individuals on the topic. A complicit society who does not question or understand the actions of a governing authority is left vulnerable, susceptible to being controlled or defined without consent. Education on how surveillance is exercised within schools, the workplace and online, is essential, in a manner which is accessible to all, to leave the decision of the legitimacy of this up to the people to regulate.

Similarly, this question carries over to the use of personal devices, such as mobile phones, laptops, or other technology, as a method used to reduce crime. In the development of the digital age, surveillance may also become a more exercisable measure, as the majority of people today hold devices which make governing bodies much more capable of reaching them. How much of our devices do we truly own, if what we do has the capacity to be tracked or recorded? Do we truly know how much of our personal data, such as passkeys like facial or fingerprint recognition, is being accessed or stored, said to be for the purpose of crime prevention? Does this have the potential to be leaked or accessed by other organisations? The unlimited questions that

arise with new technology leaves the consideration in the same way on surveillance. The files built upon our digital identities, such as past email addresses or passwords, hold valuable personal data which we may not even realise is stored. Surveillance is entirely possible in this way, of the usual time one may leave their house, tracked by location settings, to even the interests and hobbies people may have. This digital identity seems harmless and insignificant, until a governing body may know your political views, financial difficulties or even oppositions to policies. Data is stored and could be accessed from anything: text messages, bank accounts, camera rolls. How far would we be willing to share our personal data, before what may seem harmless becomes an infringement on liberty, all labelled as security measures under surveillance? We must regulate the ownership of personal data on devices, ensuring there are limits in place that maintain privacy as individuals.

The potential for surveillance to become a loose term is a large consideration we must take into account. Not only on our personal devices, but within the public domain also - through security cameras or other measures - there is the possibility for corruption. The value that personal data holds is huge, which may be even larger for corporations, businesses or political parties that could profit off of this. For example, if it was claimed that financial data was being recorded to track the frequency of theft in a local area, this type of surveillance may be passed off as a measure to prevent crime. However, a local loan company who buys access of this data could immorally target a cohort of people who are struggling to cover their bills, had they had access to their financial situations, raising profits with desperate clients. The capacity for corruption or misuse of data, labelled as a reason to prevent crime, is a major issue that, as a society, we may struggle to truly regulate. By allowing such surveillance, we may run the risk of affording too much power to a governing body, which may then create relations with other businesses who intend to use the data for alternative reasons. When the monitoring of our data and identities becomes a transactional measure, we reduce our own privacies and freedoms as individuals, through handing over the property of data we hold ourselves to other organisations.

To conclude, surveillance is a useful tool which may be used upon a society to maintain order, law and limit crime, through a series of methods. However, what maintains the legitimacy of any surveillance is its transparency, and the value which it holds explicitly, rather than as a means to obtain currency in data to trade or sell. Privacy under government is an essential requirement which allows all people to remain separate entities, although surveillance has the potential to threaten this privacy and ownership of personal identity, by exploiting this through uses that are less morally just than to simply monitor crime. It is true, that surveillance plays a major role in the deterrence,

regulation and punishment of criminal activity in society, used every day as evidence for wrongdoing. However, it is the bounds which seem non-existent in this context which push its legitimacy; to record criminals is to record the identities of all members of society, investigate them, then select what is useful or not. The majority of people are unaware of how their data could be being used in public or in private, making the population more susceptible to the immoral use of surveillance. Therefore, not only should transparency become a more significant aspect of surveillance, but education of all members of society should also accompany this, if we are to ensure that what could be done with our data is acceptable.