Task A

1. Mobile tracking works by using a variety of sources, including cellphone towers, Global Positioning System (GPS) signals, and Bluetooth beacons.

Describe in the table below how each one is able to track us through data.

|  |  |
| --- | --- |
| **Source** | **How does it work?** |
| Cellphone towers | Mobile phones connect their users to telecommunications and internet networks through cell towers. As a mobile phone moves with its user, the phone pings nearby cell towers (or “cell sites”). |
| GPS (Global Positioning Systems) | A mobile phone’s GPS capabilities allow it to track its location to within 5 to 10 feet (1.5 to 3 meters). Many smartphone apps (including maps, social media, games, shopping, and utility apps) log this location data, which can then be obtained by governments and data brokers. |
| Bluetooth | This is a wireless, low-power, short-distance set of protocols used primarily to connect devices directly to each other in order to transfer data. Bluetooth can only communicate with devices that are nearby (approximately 33 feet or 10 meters). Unlike cell tower or GPS data, which track actual location, Bluetooth tracks interactions. |

1. Using the table below, identify how these pose a threat to our data and suggest a way to ensure the data remains private.

|  |  |  |
| --- | --- | --- |
| **Example** | **Why is this a threat to the privacy of our data?** | **What can be done to ensure the data remains private?** |
| Social networking sites | They will keep track of interaction that takes place. | Know how to use privacy settings.  Be aware of how much personal information you share on your profile. |
| Spyware | You could be tricked into downloading it and allowing others to spy on the information stored on your device/computer. | Use up-to-date anti-malware software and be careful when downloading software that may look legitimate. |
| Search engines | They record information about your searches such as IP address, time spent searching, search queries made. This could make it easier for hackers to gain user’s personal identity and steal it. | Sign out of relevant accounts, especially on public computers. |
| Hackers | Gain unauthorised access to your digital devices and access your personal information. | Use firewalls, passwords and encrypt information across networks. |
| Identify theft | Involves someone pretending to be another person by collecting information about their identity. | Keep all personal information safe and secure. |
| Cookies | Small text files stored on your computer and they can store your browsing habits and websites you regularly visit. This leads to ads appearing that match your browser activity but can be seen as a privacy issue. | Know how to delete and manage cookies. |
| Geotagging | People may post photos online, such as social media and link names or other information with the photo. This can be considered an invasion of privacy. | Educate friends about the risks associated with this. |

Task B

1. Use the internet or prior knowledge to answer the following questions.
2. How does facial recognition work?

|  |
| --- |
| Facial recognition uses measurements taken between key points on the image of a face. These can be turned into ratios. For example, the distance between the pupils of the eyes (blue line) divided by the width of the nose (red line). |

1. Many high streets are equipped with facial recognition cameras however, some people believe this is an invasion of privacy.

Discuss the impact of using facial recognition cameras in public. (Looking for positive and negative thoughts)

|  |
| --- |
| Positive  It could be a good way of tackling crime because it can be a good way of detecting criminals as long as the system is accurate enough to detect faces correctly.  Negative  There could some psychological effects of the general public if they feel like they’re being watched and under surveillance and they would feel this is an infringement to their right for privacy.  Answers may vary but encourage students to provide a balanced discussion. |

Task C

1. Read the following article to answer the following questions.

<https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public?fbclid=IwAR1LJxe-Tgf3bXQ5yn6LycYcCu1m4le-isCr34LRNFhy-eAn-WUgEamqNhI>

1. What were councils given permission to do?

|  |
| --- |
| Councils were given permission to carry out more than 55,000 days of covert surveillance over five years, including spying on people walking dogs, feeding pigeons and fly-tipping. |

1. How was this evidence collected?

|  |
| --- |
| Secret listening devices, cameras and private detectives. |

1. What did the freedom of information request reveal?

|  |
| --- |
| * Checking up on benefit claimants. * Checking up on people who claim to be single parents. * Crack down on anti-social behaviour. * Monitor the sale of alcohol, tobacco and fireworks to people underage. * Capture those illegally dumping waste in recycling centres. |

1. Discuss whether you believe these councils were acting ethically.

|  |
| --- |
| The responses will vary and you may find students angle towards one side of the argument. Some might say that they’re acting unethically because it’s an invasion of privacy and so-called infringement of civil liberties.  Some might argue that what they’re doing is ethical because they’re doing everything they can to protect law-abiding individuals and deal with the minority who continuously bend the rules, therefore creating a safer community who will feel more re-assured. |

1. What is the purpose of the Investigatory Powers Act?

|  |
| --- |
| It makes provision for the retention of internet connection records for law enforcement to identify the communications service to which a device has connected. |

1. What does the act include detail of?

|  |
| --- |
| * Interception of electronic communications such as email and phone calls. * Data traffic over a network (i.e. the internet) * Surveillance * The use of undercover agents * Access to encrypted data |

1. Identify the consequences for breaking this law.

|  |
| --- |
| Penalty/Fine, Warning |