Is Mass Surveillance Moral?

Mass Surveillance is the close observation of an entire population or large group within a nation. Mass Surveillance has often been necessary in the modern era in order to fight terrorism, protect national security or fight cybercrime, like child pornography and hacking. Government groups like the UK’s GCHQ and the US’ NSA all gather information of the population of their respective country. However, arguably, it is against our human rights, specifically our human right to privacy and creates a censorship on thought. This poses the question of whether Mass State surveillance is moral or not. Arguably, it is necessary to combat terrorist groups like ISIL or domestic terrorism, in order to make the country safer. However I can also be argued that collection of data can be abused in the wrong hands, for example a change of government or stealing of the said data. Fundamentally, Mass Surveillance is immoral in that it violates an individual’s human right to privacy.

It is arguable that Mass Surveillance protects countries from a large range of threats ranging from the threat of terrorism to the threat of espionage. One GCHQ employee talked about their time as a trainee Counter-Terrorism analyst following the 7/7 attacks in London. “Following the attacks I was moved in to the Target Development team within CT- my role was to take a closer look at individuals that had been identified by the Security Service (MI5) as a possible threat. Specifically, my focus was on Al-Qa’ida (AQ) networks based abroad, who were planning attacks against the UK” [1] This statement suggests that GCHQ employees work closely with security services to prevent attacks on the UK and investigates into terrorist organisations to learn about their planned activities. This means GCHQ, and by extension Mass Surveillance, protects us from terrorist attacks and investigates terrorist organizations, which prevent future attacks.

As well as protecting the country from terrorist attacks, they also protect the country against cyber-attacks. This includes, attacks from individual hackers to organized state sponsored attacks. Another positive effect of Mass Surveillance is that it deters wrongdoers to take actions due to the fact that they are likely to be caught and know about the risks. This is evidenced by the fact that deaths from terrorist attacks and numbers of terrorist attacks in Western Europe are down from before mass surveillance. However, arguably, this is main due to decreased actions from IRA groups and lately there has been a rise in Islamic terrorist attacks in the west. The American National Security Agency, reported prevented “dozens of terrorist attacks” throughout they’re years of operation. National Security Agency Director Gen. Keith Alexander told the committee “*In recent years, these programs, together with other intelligence, have protected the U.S. and our allies from terrorist threats across the globe to include helping prevent the terrorist -- the potential terrorist events over 50 times since 9/11,*"[2] This suggests that surveillance is positive because again, a surveillance agency has been working to protect the nation against aggressive groups who are targeting the country. The prevention of 50 attacks saves the lives of hundreds of people in the United States, proving that mass surveillance prevents terrorist attacks by rooting them out by the source.

Although Surveillance agencies like GCHQ do intercept communication, it does this following the law. “*Interception of communications operations are authorised under the Regulation of Investigatory Powers Act 2000(RIPA). Warrants authorising interception can only be issued by a Secretary of State. Before an interception warrant can be issued the Secretary of State must believe that a warrant is necessary on certain, limited grounds and that the interception is proportionate to what it seeks to achieve.”[3]* This suggests that the powers of GCHQ are still limited to the law, and they do not monitor without a legal warrant from the Secretary of State meaning the usage of GCHQ is significant in such a situation. This source comes from the GCHQ website so it can be assumed they would not publish something negative about themselves, and that the information present is accurate due to them being a highly important government facility.

Government surveillance organisations can also protect a country against other countries. British organisation, GCHQ defends the country from foreign states in a different way than assisting the military. Most commonly accused of targeting the UK is Russia, either from the Soviet Union or from the modern Russian Federation. Ciaran Martin, the chief executive of the National Cyber Security Centre - a part of GCHQ, said he couldn’t “get into too much of the details of intelligence matters, but I can confirm that Russian interference... has included attacks on the UK media, telecommunications and energy sectors.” This implies that foreign interference is real and, specifically, Russia is targeting media, communications and energy in the event of a cyber-attack. This protects us as without a good cyber defence, hostile states could takedown media, communications and energy within the country, which could bring the whole country to a standstill. In the modern era we rely greatly on electrical equipment for all parts of life and increasingly media is being sent to us via mobile phones and other smart device; an attack on such technologies could bring the country back several years. Martin is the chief executive of a sector of GCHQ so it is understandable that he is well informed about the threats of cyber-attacks towards the country. However, it can be argued that this type of activity by security organisations is not related to mass surveillance of their own population as the attacks are coming from outside the country and not from the people within. This makes mass surveillance unnecessary if the threats are coming externally.

Another benefit of mass surveillance is for research purposes. The information composed for the purpose of security could also be used in the long run to better understand other aspects of society. The databases could be made accessible in the future to social scientists who could make great contributions in their fields. It will make opinion polls a lot easier to understand and could lead to the creation of a direct e-democracy via the usage of computers or mobile phones.

It can also be argued that Mass Surveillance in today’s society is not necessary and a violation to an individual’s human right to privacy. In 2015, documents from U.S. National Security Agency whistle blower Edward Snowden revealed that British Agency GCHQ had carried out mass internet surveillance in the UK under the code name KARMA POLICE (named after the Radiohead Song of the same name). The Intercept reported “One system builds profiles showing people’s web browsing histories. Another analyses instant messenger communications, emails, Skype calls, text messages, cell phone locations, and social media interactions. Separate programs were built to keep tabs on “suspicious” Google searches and usage of Google Maps.”[5] This suggest that GCHQ is gathering people’s personal and private information to create incriminating profiles of them. This isn’t protecting the individual as it is gathering private information about people’s computer. However it is possible to use the argument that only criminals should worry about being monitored and that other mustn’t worry. Conversely, it is an intrusion on an individual’s personal life by the government while could be seen as totalitarian in the same vein as a country like the People’s Republic of China and their wide spread censorship and monitoring citizens.

In the same document by Edward Snowden, It was revealed another computer system used by GCHQ, with the code name Tempora was being used to buffer Internet communications that are extracted from fibre-optic cables, so they can be processed and searched at a later time. The Guardian wrote an article saying “The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate.”[6] This is suggesting that GCHQ aim is to secretly gather information about every single person in the country secretly and have as much data about them as possible. This doesn’t protect the individual as their personal and private data is at risk in the event of a cyber or physical attack on the organisation. Although, it is possible to argue that fundamentally, gathering data on citizens in the modern world is necessary in order to find terrorists and criminals. This view fails to address that GCHQ’s Mass Surveillance has been challenged in the European Court of Human Rights after it was revealed that GCHQ had implanted intercepts at key global locations of fibre-optic cables allowing the agency to store internet traffic. Scarlet Kim, legal officer at Privacy International, stated: "These practices are unlawful and violate the fundamental rights of individuals across the world, assailing privacy and chilling thought and speech. They are incompatible with open and democratic societies." This is suggesting that mass surveillance is not appropriate to be in place in the UK as it is a democracy which aren’t compatible with the mass surveillance. All of these sources so far reference Edward Snowden, former CIA employee who copied and leaked classified information from the National Security Agency in 2013. The sources from the leak itself can be considered accurate because they are directly taken from US security agencies but the news publications that published the leak will have their own personal political orientation and put forward their own opinion within the article.

A series of documents coming from whistle-blower website WikiLeaks known as Vault7 exposes the activities and capabilities of the United States Central Intelligence Agency in electronic surveillance. The documents include details on the agency's software capabilities, such as the ability to compromise cars, smart TVs web browsers, most smartphones and most computers. WikiLeaks stated “*Most of these lagging companies have conflicts of interest due to their classified work with US government agencies. In practice such associations limit industry staff with US security clearances from fixing holes based on leaked information from the CIA*.” [7] This suggests that companies have been working with surveillance organisations like the CIA to provide backdoors for them to monitor the traffic and activity. This is immoral as it violates the trust a consumer has with the companies by providing access for government surveillance. Additionally, in the even someone finds the exploit in the software or device, it allows cybercriminals access to personal data which can be used maliciously. It can be argued that with the exposure of this information by WikiLeaks, the chance of cyber criminals finding the exploits is greater than before. The CIA released a statement saying, "*The American public should be deeply troubled by any WikiLeaks disclosure designed to damage the Intelligence Community's ability to protect America against terrorists or other adversaries. Such disclosures not only jeopardize US personnel and operations, but also equip our adversaries with tools and information to do us harm*."[8] This statement is agreeable if we consider the fact that cybercriminals and terrorist organisations can now both use the exploits the CIA used and avoid them due to the intelligence gained. However, it can also be considered that the leaks help the software companies learn about the exploits and fix them, protecting peoples personal data, like for example Mozilla which worked to fix the exploits with the provided information in an effort to protect consumers.

[1] <https://www.gchq.gov.uk/features/threat-terrorism>

[2] <https://www.washingtonpost.com/news/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/?utm_term=.595db00c3644>

[3] <https://www.gchq.gov.uk/features/gchq-oversight>

[5] <https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/>

[6] <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

[7] http://thehill.com/policy/cybersecurity/324749-assange-chastises-companies-who-havent-responded-to-cia-vulnerability

[8] <http://uk.businessinsider.com/cia-responds-to-wikileaks-disclosure-2017-3?r=US&IR=T>