To What Extent Should the Government be Allowed to Invade People's Privacy in Order to Prevent Cybercrime?

Contents

Introduction

The question I am researching for my EPQ is "To what extent should the government be able to invade people's privacy in order to prevent cybercrime?". I chose this project because the influence computers and the internet have on people's everyday lives is what makes cyber security such an important subject; the constant potential of new technologies and discoveries is one of the many things that draws me to it. Growing up in the modern world we use computers daily which has fuelled my curiosity into how computers work and how they can be used to improve the world we live in but also the negative implications that this may have.

The aim of this project is to research how much the UK government can already access our personal information, the effect this has on our day-to-day lives and how the government being able to access this information helps to keep us safe. In order to answer my question I will look at both sides of the ethical and political arguments surrounding cyber security and privacy with the aim of providing a balanced argument and to draw a fair conclusion from the information that I find.

Cyber Security

The meaning of cyber security is the 'measures taken to protect a computer or computer system (as in the Internet) against unauthorized access or attack' [1]. Since in the modern world we use computer systems and the internet daily this definition highlights the importance of maintaining cyber security by preventing cybercrime. Cybercrime is defined as 'a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes etc.). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for

communication with each other and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.' [2]

There are many different forms of cyber-crime that need to be dealt with in different ways for example:

- phishing: using fake email messages to get personal information from internet users;
- misusing personal information (identity theft);
- hacking: shutting down or misusing websites or computer networks;
- spreading hate and inciting terrorism;
- distributing child pornography;
- grooming: making sexual advances to minors. [3]

Some of these examples can be dealt with without invading people's privacy however the last three points can only be prevented by viewing internet users personal data for example their private conversations to discover these crimes. This creates a moral dilemma resulting in arguments over whether our government should be able to access these conversations to stop these crimes or if this is a violation of our human rights.

Nowadays, all digital devices (including computers, tablets, and smartphones) are connected to the internet. 'In theory, cyber criminals could bring a large part of the country to a halt. The government rightly takes cybercrime very seriously, and are working hard to fight it.' [4] In order to keep us secure cyber security laws are put into place to protect us and to control what happens with our data.

Laws and Rights

Currently there are multiple legislations in the UK regarding cyber security including:

- The data protection Act (1998) which is designed to make sure that personal data is kept up-to-date, safe, secure and not used in ways that would harm individuals.
- The Computer Misuse Act (1990) which makes it an offence to access or modify computer material without permission.
- The Regulation of Investigatory Powers Act (2000) which regulates the powers of public bodies to carry out surveillance and investigation and cover the interception of communications. [5]

There are many challenges facing legislators when it comes to cyber security because of the rapidly changing field of computing and worldwide communications. New applications in computing are constantly being invented and with them new ways of committing offences for which there is no legislation. This means that legislators have to balance the rights of individuals with the need for security and protection from terrorist or criminal activity. This has resulted in many countries restricting or banning the use of strong cryptography (the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text [6]) which gives the government access to more personal information.

The regulation of investigatory powers act enables:

- Certain public bodies to demand that and ISP (internet service provider) provide access to a customer's communications in secret.
- Mass surveillance of communications is transit.
- Certain public bodies to demand that someone hand over keys to protected information.
- Certain public bodies to monitor people's internet activities. [7]

This means that under current laws the UK government should be able to access any personal information needed to prevent attacks and keep us safe but the act also prevents the existence of interception warrants and any data collected with them from being revealed in court. This should mean that officials could intercept data to detect and prevent crime however; people do not need to worry about their private information being revealed in court. Unfortunately, in reality this often means people get away with crimes they committed online since they cannot be charged with enough evidence.

Another issue with cyber security laws is that different countries have different laws and it is often hard to prove which country an offence was committed in and equally hard to trace the offender or to prosecute them. This means that in many cases it is only the data of innocent people that is collected whereas criminals figure out ways to hide this information from officials. The effect this has on our privacy means many people are too afraid to speak freely online since records are being kept of everything that they do which could result in people losing their jobs or even facing jail time many years later over minor offences.

Cyber Attacks

A cyber-attack is "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm" [8] and with the rapid increase of cybercrime occurring each year it is essential that cyber security professionals are keeping up with the development and learning how to prevent and recover from these attacks.

'Just over 51% of the world's population currently uses the internet and this is expected to increase to 75% by 2022 and 90% by 2030… it is estimated that by 2020 a business will fall victim to a ransomware attack every 14 seconds' [9] which highlights the importance of keeping our data safe. This increase in internet use has resulted in cyber-attacks becoming the most profitable form of crime beating the global trade of all illegal drugs and these numbers are only set to rise.

One of the major obstacles when it comes to preventing cyber-crime is that cyber security professionals generally work 9-5 jobs and have to follow set regulations whereas cyber criminals can be active 24/7 and their methods of attacks are always evolving quicker than companies methods of defense can.

"Cyber attackers constantly evolve their skills and will always find new ways to attack—it's not a question of if, but of when." —Eileen Dignen (2018)

“If your data is valuable enough, there is almost nothing you can do to provide total security against an expert adversary. Simply put, the attacker may be smarter than anyone you have defending the network. Cyberattacks are not only impossible to block, they're often difficult to detect; you may not even know you're under attack in the first place.”—Robert W. Lucky (2018)

The importance of maintaining effective cyber security has been demonstrated by multiple cyber-attacks such as the WannaCry hack, which shut down hundreds of thousands of computers around the world with messages from hackers demanding ransom payments. This majorly effected the NHS causing “more than 19,000 appointments to be cancelled, costing the NHS £20m between 12 May and 19 May and £72m in the subsequent cleanup and upgrades to its IT systems” [10]. At the time of the attacks, the NHS was criticized for using outdated IT systems, including Windows XP, a 17 year-old operating system that could be vulnerable to cyber-attacks. This is an example of an attack that could have been prevented without any further personal data being accessed however finding and prosecuting the attacker to prevent them from reoffending would be easier if officials had access to more data which could ultimately prevent another attack and stop peoples private data being made public or held for ransom.

In other cases more could be done about cyber-attacks if the government had access to more private information for example in the US the FBI needed Apple to unlock a suspected criminals iPhone which would enable them to prosecute the criminal and prevent further attacks. Apple specifically altered its software in 2014 to ensure that it would not be able to unlock customer phones and decrypt any of the most important data on them; but it turns out it overlooked a loophole in doing this that the government is now trying to exploit. The loophole is not about Apple unlocking the phone but about making it easier for the FBI to attempt to unlock it on its own. “If the FBI is successful in forcing Apple to comply with its request, it would also set a precedent for other countries to follow and ask Apple to provide their authorities with the same software tool” [11] . This would mean the government would always be allowed to access user’s personal information without permission resulting in a major reduction in privacy.

The chief of the national cyber security center in the UK warns that there is “little doubt” that a major life-threatening cyber-attack will occur in the UK and that “these groups constitute the most acute and direct cyber threat to our national security” [12] . Because of these threats, the UK has plans to implement mass surveillance both online and in the real world to help prevent attacks. Mass surveillance can have a huge negative impact on people lives and the European Court of Human Rights has ruled that it will “violate human rights laws” [13] however if the UK leaves the EU the government will most likely no longer have to follow these rules. Bernard Keenan, a lecturer in law at Birkbeck, University of London says, “Secrecy has always been put on a higher footing than legality in the history of the British state” so it is likely that the UK government will continue to put national security above personal privacy.

On the other hand, for many people surveillance makes them less safe: it is not the security blanket politicians are holding it up to be. Job seekers under surveillance can lose income

needed to survive if their online activity fails to match up to job search demands. People interested in campaigning hesitate over getting involved with movements for social justice when the police count activism as akin to domestic terrorism. It is clear that surveillance affects a broad group of people, with real painful consequences for their lives. We have seen journalists being monitored, lawyers having their client confidentiality broken, victims of police misconduct being spied on and environmental campaigns infiltrated. These people are not criminals, and yet when we have a system of mass surveillance, they become targets for increasingly intrusive powers. Edwards Snowden who exposed the NSA for collecting phone records of millions of Verizon customers daily stated, “For many kids, the internet is a means of self-actualisation. It allows them to explore who they are and whom they want to be, but that only works if we are able to be private and anonymous, to make mistakes without them following us. I worry that mine will be the last generation to enjoy that freedom. I do not want to live in a world where we have no privacy and no freedom, where the unique value of the internet is snuffed out”. [14] This is the main argument people have against increasing surveillance however many of these people would likely change their mind about it if a crime is committed against them and breaching a suspects privacy is needed for justice to be served.

Technological Advancements

As technology advances our security systems will need to adapt with it. This is likely to result in further surveillance as the wold becomes more automated which will have a drastic effect on our privacy. Many people are excited about driverless cars, smart homes, AI and more but most of them just want the latest tech and do not stop to think about the safety of it. This is why Jeff Lipton, vice president of WaterSmart in San Francisco, a company that makes connected programmable water meters, thinks "these systems need to be very carefully thought through before rushing to make every device in a city smart". It is not just the devices themselves that are vulnerable - the network potentially is, too. If hackers gained access to these systems, they could potentially find out everything about a person’s life or even control people’s smart home devices. An example of this is the website http://www.insecam.org which is the “biggest directory of online surveillance security cameras” [15] allowing users to search live web cams around the world. Most of these cameras view streets and other public places however; some show footage from within people houses.

Although websites like this sharing other peoples’ personal information is illegal in most countries it is extremely difficult to monitor due to the sheer number of sites on the internet and this number is only going to increase. "Google and Facebook spend billions on security and both have recently been hacked," says Mr Burstein. "If they can't be fully protected, how can an ordinary person be expected to secure the dozen or more connected devices many of us will soon have?" [16]

Because of the high demand and competition for new technologies, many companies try to release new products without evaluating the security risks in enough detail. For example Adam MacHale, managing director of technology strategy at IT and networking firm Cisco

Systems says "With 5G we'll be consuming services from all over the place, so we want to deliver those services very quickly as close to the customer as possible to reduce latency (delay)". People caring more about efficiency and having the best tech do not focus enough on security and safety which will likely result in their data being stolen which could be used against them in the future.

Many films and TV programs have tried to predict the future of technology for example in 2016 the Black Mirror episode 'Nosedive' was released showcasing a dystopian future where everyone rates the people they meet from one to five stars after each of their encounters or on social media posts. This resulted in a world where everyone acts with false positivity, became social media obsessed and having a negative rating could prevent people from doing certain things in the real world like living in certain places or applying for certain jobs. At first, a world like this seems greatly over exaggerated but countries like China are already beginning to implement a similar social credit system.

The "social credit system," first announced in 2014, aims to reinforce the idea that "keeping trust is glorious and breaking trust is disgraceful," according to a government document. The program is due to be fully operational nationwide by 2020, but is being piloted for millions of people across the country already. The scheme will be mandatory. Like private credit scores, a person's social score can move up and down depending on their behaviour. The exact methodology is a secret but examples of infractions include bad driving, smoking in non-smoking zones, buying too many video games and posting fake news online. [17]

Although this system has not yet been fully implemented, some citizens have already been punished for having low social credit scores. Examples of these punishments are:

- Restricting Travel – Nine million people with low scores have been blocked from buying tickets for domestic flights. They can also clamp down on luxury options e.g. three million people are barred from getting business-class train tickets. [18] The eventual system will punish bad passengers specifically. Potential misdeeds include trying to ride with no ticket, loitering in front of boarding gates, or smoking in no-smoking areas.
- Throttling your internet speeds – Although the exact mechanics of this punishment have not been defined yet it is likely that spending too long playing video games, wasting money on frivolous purchases and posting on social media will result in this. Spreading fake news, specifically about terrorist attacks or airport security, will also be punishable offences.
- Banning your children or you from good schools – This would mean that the social credit system will be used on minors as well as adults and you could be effected by the social credit score of the people associated with you. Already In July, a Chinese university denied an incoming student his spot because the student's father had a bad social credit score.
- Stopping you getting the best jobs – It is not yet clear how this punishment will work but "Trust-breaking" individuals would likely be banned from doing management jobs in state-owned firms and big banks.

- Keeping you out of the best hotels – People who refused military service have been denied access to some hotels and people with good scores can speed up travel applications to places like Europe.
- Getting your dog taken away – 'The eastern Chinese city of Jinan started enforcing a social credit system for dog owners in 2017, whereby pet owners get points deducted if the dog is walked without a leash or causes public disturbances. Those who lost all their points had their dogs confiscated and had to take a test on regulations required for pet ownership.' [19]
- Being publicly named as a bad citizen – although this punishment has not yet been implemented there are plans to create a blacklist of citizens so that companies can consult the blacklist before hiring people or giving them contracts.

Currently this social credit system is only being implemented in China however many people believe the UK and other western countries will eventually follow suit. There are many positive impacts of having a system like this because it encourages good behaviour however it is an extreme invasion of privacy and making one mistake could affect you forever. "Despite the creepiness of the system Human Rights Watch called it chilling, while Botsman called it a futuristic vision of Big Brother out of control — some citizens say it's making them better people already" [20]. Many Chinese citizens say they like the idea of having a social credit system because having a good score gives them benefits for example getting more matches on dating websites, discounts on energy bills, renting things without deposits, and getting better interest rates at banks.

This is an example of a government-invading people's privacy in order to obtain cyber security also resulting in the government taking control over what its citizens can do and say. Although the benefits of this system may make it look like a good idea, it will result in people not being able to speak freely against the government or the social norm without being punished meaning they are forced into silence preventing human rights and social justice movements. On the other hand many people argue that the social credit system is just a more advanced version of systems we already have like financial credit and people can already be kept on blacklists for crimes they have committed preventing them from getting certain jobs.

Free Speech vs Hate Speech

For many people the internet inspired a generation to voice a broad diversity of opinion and empower those who traditionally had no voice and in many cases, this has been a success. On the other hand, because of this freedom online trolls, cyber-bullying and misogyny have become a fact of everyday life on the internet. Feminist writers and journalists, academics like Mary Beard and political campaigner Caroline Criado-Perez , who petitioned the Bank of England to create a bank note featuring Jane Austen's face, receive hundreds of death threats, rape threats and other offensive communications for no other reason than that they are women who have dared to appear on the media. Detectives from the MPS have arrested a 32-year-old-man, on suspicion of committing an offence under the Protection of

Harassment Act, 1997 for making these threats on twitter [21]. Thousands of other women and teenage girls are victims of similar trolling on the internet. Savage bullying on various social networking sites has led to several tragic cases of suicide.

The internet has brought great benefits but all of us have a responsibility to use it wisely and well. This has resulted in the argument of free speech vs hate speech being one of the major issues facing social justice activists today. Under Article 10 of the Human Rights Act 1998, "everyone has the right to freedom of expression" in the UK. Nevertheless, the law states that this freedom "may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society". A number of different UK laws outlaw hate speech. Among them is Section 4 of the Public Order Act 1986 (POA), which makes it an offence for a person to use "threatening, abusive or insulting words or behaviour that causes, or is likely to cause, another person harassment, alarm or distress". This law has been revised over the years to include language that is deemed to incite "racial and religious hatred", as well as "hatred on the grounds of sexual orientation" and language that "encourages terrorism" [22]. Many people have an issue with this law because whether something you say is considered hateful depends on people's reaction to what you say which is very unpredictable and policing speech makes people afraid to express new ideas.

On the other hand, complete freedom of speech including hate speech can result in the spread of radical ideas. For example, after the 2010-11 Arab Spring, many people argued that the social media networks were helping to overthrow dictatorships and empower the people but it deteriorated into vicious religious and ethnic civil wars culminating in the rise of ISIS, which uses social networks to post atrocities and radicalise impressionable young people [23]. Hate speech can result in people feeling unsafe online and even committing suicide over negative comments. To combat this the government can read peoples private conversations to ensure they are not being radicalised or abused however, this also causes ethical issues because of the invasion of privacy.

Multiple people in the UK have been arrested or punished over things they said online that they meant to keep private because it could be considered hateful. Some individuals are outraged by the invasion of privacy carried out to protect us online but others respond with the common phrase "If you have nothing to hide you have nothing to fear". There are many arguments over the validity of this phrase for example Edward Snowden, US government whistle-blower and former NSA worker believes "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say". Whereas Eric Schmidt, the CEO of Google said "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" [24].

This powerful phase does many things such as encouraging a complete trust in state powers suggesting that you will never face wrongful suspicion or misuse of powers, for 'only the guilty are affected by mass surveillance'. It encourages people to embrace their own innocence, to look inwards, and not to look at how other people have been treated or targeted. It also introduces the vague threat if you have not behaved, you do have

something to fear. Not something to challenge, or criticise, but to fear and so it keeps us in our place. This can have a negative effect on many people for example:

- Victims of police misconduct could be surveilled in attempts to smear them and undermine their fight for justice.
- MPs need privacy in particular for their constituency work, which involves meeting with people who share very personal stories and situations, and challenging the actions of the government. For example, recently MPs confidential calls with prison staff were recorded and monitored.
- Journalists are frequently at risk of big business and government surveillance tracking their leaks, their stories, their whistleblowers, and their criticism of the government and the police.
- Whistle-blowers cannot expose wrong-doing, whether by the state or powerful businesses, in a world that always watches, but are meant to have special protections.
- Lawyers rely on client confidentiality, a principle that is key for a fair trial, and for a working justice system. [25]

Although the government claims to have good reasons for increased surveillance, many people fear that they could also use this power to manipulate citizens and exploit the information they can gain access to in other ways. Because of this, many people resort to finding their own ways to protect their privacy online.

Protecting Privacy Online

As I mentioned earlier the UK has a law called the Investigatory Powers Act (2016) that more or less removes your right to privacy online. This means that your ISP has to give the government information on your internet use if asked for it. There are multiple methods people use to attempt to prevent this.

One of these methods is use of a VPN (Virtual Private Network). By using this while browsing online traffic from your PC is automatically encrypted and sent to the VPN supplier's server, so your ISP can't see the final destination. [26] This means that the government can still ask your ISP for your personal browsing history but the ISP will not have been logging your web visits. Issues with this method are that your browser is still tracking your browsing and so are advertising services, also governments would likely still be able to gain information on you if they needed to. Encrypted messaging apps such as whatsapp could also be used for more privacy but this has the same issues.

In the past use of proxy servers and VPNs were a red flag to the government since it suggested cyber-crimes were being committed however in recent times people to protect themselves from cyber-attacks commonly use them. [27] This is another reason against increased invasion of privacy in the name of cyber security since many people view it as their own responsibility to protect themselves from hacking by limiting the amount of data they make public on social media and by making use of these methods. Additionally, in

many cases cyber criminals know how to avoid government detection so serious criminals can still get away with crimes and only normal innocent citizens are effected by the surveillance. On the other hand, many people argue it is unfair to leave internet users to defend themselves again cybercrime since it is not their responsibility to protect themselves from criminals and many people do not have the expert knowledge required to do this effectively on their own. They are willing to sacrifice some of their privacy if it means keeping themselves safe online.

Conclusion

There is no clear answer as to what extent the government should be able to invade people's privacy in order to obtain cyber security but it all comes down to whether the drawbacks of reduced privacy are outweighed by the benefits this has in helping to protect us from cyber-crime.

When allowed access to peoples personal data the government seems to be very effective at stopping major cybercrime. For example, you may think most terrorists going through airports are stopped at airport security however in reality "95% of terrorists can get weapons through airport security" but most of these attacks are prevented by cyber security intercepting the terrorists' communication. [28] On the other hand law enforcement are not as effective at tackling more minor cybercrimes such as piracy, hacking and spreading of hate speech which are the things that tend to effect individuals everyday lives.

Some people argue that the government should not try to protect us from hate speech since they believe it is a part of free speech and that if you make it illegal to say extreme views people will continue saying it in more private places, which is potentially more dangerous. However, even in countries with freedom of speech laws companies online decide what is allowed in their platform and will mostly only include content deemed advertiser friendly which should keep the general public safe from hate speech and help to prevent people from spreading it or being manipulated by it.

In conclusion, I believe that the government should be allowed to invade people's privacy when it is required to prevent crime or for prosecuting cyber criminals however, these powers should be regulated to ensure the government do not overstep these boundaries allowing them to gain too much control over the public like what has happened in China. I also think that people need to be educated on how to keep themselves secure online since technology is becoming an increasing importance in our lives. The vastness of the internet means that law enforcement cannot control all cyber-crime on their own so people should take their own precautions when using modern technology.

Bibliography

[1] Definition of cyber security (https://www.merriam-webster.com/dictionary/cybersecurity, 2018)

[2] Definition of cybercrime (techopedia.com, 2017)

[3] Types of cybercrime (https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/, 2018)

[4] Importance of cybersecurity (www.government.nl, 2016)

[5] Cyber security laws (https://www.thedigitalwatcher.com/uk-cybersecurity-law, 2018)

[6] Cryptography definition (https://www.webopedia.com/TERM/C/cryptography.html, 2017)

[7] Heathcote, P. (2016).Computer Science(4th ed.).Dorset,UK: PG Online Limited,

[8] Cyber attack definition (https://www.merriam-webster.com/dictionary/cyberattack, 2018)

[9] Cyber attack statisitcs for 2018 (https://www.itgovernance.co.uk/blog, 2018)

[10] NHS Cyber Attack (https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled, 2018)

[11] FBI's legal battle with apple (https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/, 2016)

[12] NCSC warnings (https://www.news.sky.com/story/amp, 2018)

[13] UK Mass Surveillance (https://www.wired.co.uk/article/uk-mass-surveillance-echr-ruling, 2018)

[14] NSA Mass Surveillance (https://www.theguardian.com/world/2013/jun/06, 2013)

[15] Website streaming private cameras (https://gizmodo.com/a-creepy-website-is-streaming-from-73-000-private-secur-1655653510, 2014)

[16] Cyber Security Advancements (https://www.bbc.co.uk/news/business-45952693, 2018)

[17] Chinas Social Credit System (https://www.businessinsider.com/china-social-credit-system, 2018)

[18] Social Credit Statistics (https://www.channelnewsasia.com/news/asia, 2018)

[19] Dogs Social Credit (https://www.businessinsider.com/china-dog-owners-social-credit-score, 2018)

[20] Chinas Social Credit System (https://www.bbc.co.uk/news/world-asia-china-34592186, 2015)

[21] Protection of Harassment Law (https://www.theguardian.com/uk-news/2013, 2013)

[22] Hate Speech (https://www.theweek.co.uk/97552/hate-speech-vs-free-speech-what-are, 2018)

[23] Keen, A. (2015).The Internet is not the Answer. London,UK: Atlantic Books,

[24] Nothing to hide arguments (https://en.wikipedia.org/wiki/Nothing_to_hide_argument , 2018)

[25] Nothing to hide arguments (https://www.openrightsgroup.org/blog/2015/responding-to-nothing-to-hide-nothing-to-fear , 2015)

[26] Protecting Privacy Online (https://www.theguardian.com/technology/askjack/2016/nov/24/how-can-i-protect-myself-from-government-snoopers, 2016)

[27] VPNs Legality (https://www.techadvisor.co.uk/feature/security/are-vpns-legal-3673180/, 2019)

[28] Airport Security (https://www.internationalairportreview.com/article/69862/threat-of-terrorism-aviation-industry/, 2018)