Surveillance

Watch The Many, To Catch The Few

George J. Thorley

Norwich Steiner School

Author Note

George J. Thorley, Level 3 Steiner School Certificate, Norwich Steiner School.

This report is the piece of work required for the Steiner School Certificate Level 3 Class 12 Project.

Correspondence concerning this report should be addressed to George Thorley, Norwich Steiner School, Hospital Lane, Norwich, NR1 2HW.

Contact: g.j.thorley@gmail.com

Contents

Summary

In this report, my main question will be: What was the extent of government mass surveillance, in particular the NSA in the United States, running from the September 11 attacks in 2001, to the Edward Snowden revelations in 2013? In answering this I will focus on how public and political feelings prompted the conditions possible for the security forces to be doing what they do in todays world. In particular, I will be looking at the National Security Agency (NSA) in the United States (US) and some of the revelations brought forward by Edward Snowden in 2013, along with the scale of involvement of the United Kingdom's (UK) Government Communication Headquarters (GCHQ). I will then look at some of the fundamental questions that surround the world of mass surveillance, such as the effectiveness of the programs that were acted upon by security agencies, who they were really looking for, and whether, in my eyes, their methods were morally right.

Keywords: NSA, GCHQ, Edward Snowden, surveillance

Surveillance

Watch The Many, To Catch The Few

Introduction

When I started my project, I was interested in the constant battle between a state and a so-called terrorist organisation. I began by considering doing a research report on whether it was possible to ever put a total end to this conflict. However, I was hampered by a problem with the way the world works. Which made it largely impossible to answer my question, or come to a satisfactory conclusion to the problem. The issue was that there is no universal definition for the word terrorism. Every situation is different, and no one refers to themselves as a 'terrorist'. Therefore to do that report I would have had to come up with my own definition and a hypothetical solution. The report would have been too abstract and would have lacked factual data.

Because of this, I decided to reform the report. With help from my supervisor, I came to the conclusion that it would be more effective to research the definitions of the word 'terrorism' and how that word manifests itself. Over the course of two terms I made plans to write this report. However, at the beginning of the Easter holidays, I came to the conclusion that I may not enjoy actually researching and writing the report. Real issues interest me.

As I was writing an English essay on the book *1984* by George Orwell, I came across an article on the Guardian website, titled: '*NSA files decoded: Edward Snowden's surveillance revelations explained*'. (Macaskill & Dance, 2013). The article showed the NSA files, revealed by Edward Snowden, in their full light. The article had a timer from the moment the reader clicked on the website, which showed how much data the NSA had collected in the time from when the reader had begun reading the article. Second by second the amount of data collected reached massive numbers and I found that very interesting and quite frightening.

As I began researching further, a fundamental question arose, which is what this report is based around: What was the extent of government mass surveillance, in particular the NSA in the United States, running from the September 11 attacks in 2001, to the Edward Snowden revelations in 2013? Throughout the journey of researching and writing this report I began developing further, more specific, questions

such as: What accountability does the government have to its citizens, and companies have to their customers? Who are the targets of mass surveillance? What is the real aim of the security forces? What is the moral acceptability of such surveillance? And finally, is this type of surveillance effective? I attempt to explore these questions throughout this report.

However, to begin this report, I have chosen to provide a brief historical context to the life of the NSA prior to 2001.

Historical Context

The National Security Agency (NSA), as it is known now, began its life right after the Second World War. However, its birth can be contributed to much earlier government spy organisations. While the general idea of spy agencies has been around for centuries, I am choosing to just go back a hundred years, to 1917. Just before the United States entered the First World War, the father of the NSA, the Cipher Bureau of Military Intelligence was formed. (Heiligenstein, 2014). After the First World War the agency "…shifted its focus from military to diplomatic intelligence." (Heiligenstein, 2014). Much like todays NSA, the Cipher Bureau began concentrating on foreign governments and message traffic entering and exiting the United States. According to the Saturday Evening Post, Henry Stimson (Secretary of State of the Herbert Hoover administration from 1929) found fault with the morality of the program undertaken by the agency, and subsequently, the agency was shut down in 1929. Stimson found that the reach of the Cipher Bureau had strayed across Constitutional lines, and had become too intrusive on the private lives of ordinary people. He figured that such an agency was better suited to wartime operations, and was therefore not needed when the United States was not at war.

A few months later, however, the military installed their own intelligence organisation, and took off where the Cipher Bureau had ended. "William Friedman began building the Signal Intelligence Service (SIS)." (Heiligenstein, 2014). SIS were used heavily during the Second World War to crack the Japanese military codes. Whether key to US victory or not, great successes were had from the intelligence gathered by SIS against the Japanese. An example of this, is when SIS intercepted communications from the Japanese Navy, making it possible for the US Navy to "… anticipate the Japanese attack on Midway in June 1942." (Heiligenstein, 2014).

In 1952, President Truman integrated and reformed SIS into the NSA. Secrecy was paramount; the agency was "…half-jokingly referred to by many as 'No Such Agency.'" (Heiligenstein, 2014). Their work was strictly a government matter, and no information was released to the public. The agency focused on the Cold War issues, hacking the Soviet government, finding missile counts (amount of missiles and armament) and spying on communications. As the two superpowers spiralled around the fringes of a nuclear war, the NSA gained employees, reaching a maximum number of 90,000 people - the largest on record. Keeping the agency secret got harder and harder.

After the Watergate scandal of 1972, where burglars were found in the Democratic National Committee during the reelection of President Nixon, public scrutiny fell onto the surveillance carried out by the NSA (History.com Staff, 2009). The Watergate scandal triggered an investigation into the security agencies, and the NSA found themselves in the spotlight. From this moment on the NSA found themselves being restricted, and mistrusted. The investigation revealed that: "Since 1945, the NSA had been spying on telegrams entering and leaving the U.S., including the correspondence of American citizens, under a program called Project SHAMROCK." (Heiligenstein, 2014). This showed to the US citizens that the NSA could well have been spying on their communications for government purposes. It now became clear that there needed to be a system to prevent the President, or the NSA, from spying on US citizens. The mistrust that was felt towards the agencies has never left. The covert operations present in the Watergate scandal placed a black mark against the agency, and public feeling towards the agency has been one of mistrust and suspicion.

A reaction to this investigation came in 1978 when the US government introduced the Foreign Intelligence Surveillance Act (FISA), which curbed mass surveillance by the NSA on US citizens. From then on, the idea went, security agencies would be monitored, and censored by a specially formed court called the Foreign Intelligence Surveillance Court (FISC). Warrantless wiretapping was stopped and secrecy of what the agency did was shown to the public, so for a period of around 23 years the NSA and all security forces were held to account, they bided by the law, and were watched closely by Congress and the FISC. Ironically enough, 26 years later, this very same court began authorising the NSA to conduct mass surveillance, I will return to this in due course.

After the FISC had been introduced, the power of the NSA had been drastically cut, their popularity was low, the survival of the agency rested on the edge of a knife.

To regain their old Cold War privileges of Presidential support and secrecy away from the courts, the NSA needed something that would show their worth to the United States, something that would prove that they were necessary, something so big that Congress, the media and the courts would look the other way. Fortunately for them, they got just that.

9/11

On September the 11th 2001 an event took place that changed the course of history. A statement of contempt, so massive, that it brought a world superpower to its knees. The September 11 attacks on the World Trade Centre and the Pentagon turned the tide of human endeavour, and brought a new meaning to what seemed acceptable within society. As the twin towers burned, the pride of nation went up in flames. As the news flashed around the world an attitude of shock and disbelief flew with it. What had been deemed impossible became a reality. A real threat had been realised. The invincibility of the western world had been broken, and a new era of fear ensued. Fear became a massive player on the world stage in the post-9/11 world, especially in the United States. As will become apparent, fear played a huge role in how the US responded to the 9/11 attacks, and how it was used to manipulate public and political feeling.

Political reaction was quick and ruthless. The so-called 'War on Terror' was announced by President George W Bush just 11 days after the attack took place. The War on Terror gave the United States government authorisation, if you will, to take steps to prevent another terrorist attack. Counterterrorism became top priority for the Bush administration, or so they made out. After the attacks, military and political changes, which were seen as controversial, were said to 'protect the United States from the threat of Terrorism'. The invasion of Iraq, the fight against Al Qaeda, and the 10 year long hunt for Osama Bin Laden are just some of the examples of the War on Terror. And this was all accepted because the people of the United States felt genuinely fearful of further terrorist attacks. The word 'terrorism' was branded into their memories by both the government and the western media. The word became so

frequently used that its meaning became warped and gradually twisted. Taryn Butler wrote a research report on the use of the word Terrorism pre/post 9/11 and found that "…the media was much more inclined to use the word terrorism after 9/11 and the frequency in terrorism reports were a lot higher, creating a fear-inducing mindset amongst Americans." (Butler, n.d.). This mindset became a reality for the citizens of the United States after 9/11, which played a major role in the government's global counterterrorism campaign.

This mindset was helpful to the Bush administration, as it allowed them public support on all anti-terror operations. For instance, the 14 year war in the Middle East or the opening of Guantanamo Bay. Major world operations, which before 9/11 may have been questioned, were, instead, seen as necessary, in the fight against terrorism. Counterterrorism became the reason, or excuse, for any controversial government activity.

USA PATRIOT Act 2001

An aspect of this was the passing of the USA PATRIOT Act of 2001. The Patriot Act rewrote the rulebook on what the intelligence agencies were allowed to do on American soil. Non-abbreviated, the Act's name is written: 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001'. First off, it is interesting to note that an abbreviation of this title is 'PATRIOT' which is even more interesting when considering that that became how people referred to it. A patriot is someone who against all odds defends their country, and here, the Bush administration used clever psychology, so that the Act bears the same name. Also, slightly ironically, Edward Snowden could well be considered a patriot - depending how someone looked at him, he could be an enemy of the state or a patriot. This is an interesting manifestation of opposites. The patriotism behind Snowden's revelations is something that I will return to towards the end of this report.

Calling this Act the Patriot Act leads one to think that the Act is patriotic in its endeavours. I feel this may have given it an advantage as the Bush administration pushed the legislation through the House of Representatives. Just over a month after one of the most shocking acts of terrorism in modern times, the USA PATRIOT Act passed Congress with a staggering majority. Although there have been many queries since, questioning whether forcing the Act through the House of Representatives at this

time was opportunistic. David Peterson, writing for ApexCCTV, wrote: "Many opponents of the act state that the bill was enacted so quickly after the September 11, 2001 terrorist attacks, that it wasn't properly vetted in Congress and the Senate." (Peterson, n.d.). I will return to this in a moment. But right after the Act was vetted by the House of Representatives it was signed into effect by George W Bush on the 26th of October 2001.

The USA PATRIOT Act allowed security agencies to acquire warrants for wiretapping, roving wiretaps, emails, voicemails and any other forms of electronic communication, far easier to obtain. For instance, their needed to be no real tangible evidence to suggest that a citizen of the United States was involved in an act of terror, for a warrant to be easily acquired for the NSA to wiretap their phone, and intercept their communications. "All that is essentially required to begin monitoring a citizen's activity is a suspicion the person is somehow engaging in terrorist acts or felony crimes." (Peterson, n.d.). This allows the NSA or FBI to spy on any US citizen if they believe that there is a chance that their actions could be aiding a terrorist movement.

And because, as said earlier, the bill was rushed through the House of Representatives at a time when the United States was still reeling in shock from the 9/11 attacks, very little thought was put into considering if the bill was constitutional, or in fact if the Act violated the Fourth Amendment. The Fourth Amendment clearly states that in the case of searches and seizures "…no Warrants shall issue, but upon probable cause…" (Legal Information Institute, n.d.) and that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…" (Legal Information Institute, n.d.).

This leads me to question how the Patriot Act and the Fourth Amendment manage to work in the same legal system as they clearly oppose each other. Perhaps the answer to this lies in Michael Moore's film *Fahrenheit 9/11* where he famously tapes Congressman Jim McDermott admitting that no Senator had read the Act before passing it into law (Vargo, 2015). If this is in fact the case, I further question the failure of the House of Representatives, the most powerful elected protectors of the Western world constitution, failing to even read what they are signing. To me, the Patriot Act is clear violation of the Fourth Amendment, and every thing the American constitution is made to protect. For the basic rights of citizens to be compromised in this way, it makes me wonder whether the US government, at this time, forgot their main and primary

role: upholding the constitution, and working for the benefit of US citizens. In my own view, the Patriot should have been thrown out long before it became part of the law. If not by Bush, then by the Representatives, and if not by the Representatives, then the courts. Violation of the American constitution, and legal system, is something that will continually spring up throughout this report.

I came across the Patriot Act whilst watching *Fahrenheit 9/11* a couple of years ago and subsequently revisited the legal structure and contents of it while researching the legal framework which the NSA worked from. Interestingly, through research into the Patriot Act, I came across a far more intrusive, and constitutionally questionable piece of legislation that had emerged through various leaks, long after it was enacted.

Presidents Surveillance Program

On October the 4th 2001, prior to the Patriot Act becoming part of US law, President George W Bush signed an executive order called the Presidents Surveillance Program (PSP) codenamed 'Stellar Wind'. The program was then reauthorised every 45-60 days by the President up until 2004, when authorisation became a court matter. The Program authorised warrantless wiretapping and broad scale surveillance in order to intercept communications from US and non US citizens. The program was top secret; very few people were made aware of the order. Right from the start, the legality of the program was questioned, as in many ways it seemed to violate the Fourth Amendment. According to a book called *Bush's Law,* by Eric Lichtblau, the day after Bush signed the executive order, the Attorney General, John Ashcroft, was allegedly told to 'Just sign it' (Electronic Frontier Foundation, n.d.). It later emerged that Ashcroft had okayed the order without even checking its legality. Before any government lawyer had checked the legality of the program, the NSA had already begun approaching communication companies about handing over customer data. The NSA acted before even a government lawyer had seen the program, so that there was no real ratification of the program, no tick-list, no care was put into checking if it violated any existing law or the constitution. It wasn't until November the 2nd that OLC Lawyer John Choon Yoo confirmed its legality. This is known to be true as it was clearly stated in the Inspector General report published in 2009.

Again, a complete oversight of basic protocol by the United States. I stated earlier that it was the NSA that were put on a leash in 1978, but the government of the United States are the ones that are now violating their own legal system. In the end, it's the NSA's job to do as they are ordered, or authorised. This particular case, and in the case of the Patriot Act, it is the United States government who are violating the American constitution. Very briefly, I now return to the American Declaration of Independence in 1776, with a quote from that which sums up the duty of US citizens if the government begins violating the constitution: "…when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their [the peoples] right, it is their duty, to throw off such Government, and to provide new Guards for their future security." (Arnold, 2007). The Declaration of Independence is the foundation of American society, and continued violation of this, could be the beginnings of a civil war. The very act of crossing constitutional limits is meant to be beyond what a government can do. However, to protect itself, the government kept the program very secret.

By October the 16th 2001, NSA employees had approached major telecommunications companies, who were asked to voluntarily hand over customer data. The companies were told that the government "needed to identify members of international terrorist cells in the United States and prevent future terrorist attacks against the United States." (Electronic Frontier Foundation, n.d.). Bending the companies backs over the 9/11 attacks gave the NSA a good hand when prying customer's information out of large telecommunication companies. The companies complied with the NSA almost instantly, and data began flowing into the NSA's headquarters (companies later claimed that they had only acted on accordance with the law, and that customer information was never given away without extensive consideration).

A pre-Watergate scandal situation had been revived, a situation that had supposedly been laid to rest. The NSA regained what they had lost - government support and authorisation had been reinstated. The NSA could rebuild their mass collection of communications travelling via these companies.

It wasn't until the end of January 2002 that one of the eleven Judges at FISC - the court responsible for regulating the NSA, was told about the program.

According to *Bush's Law,* by Eric Lichtblau, later in 2002, an American Telephone And Telegraph (AT&T) technician found out about secret rooms being built at AT&T's office blocks around the country. The technician, allegedly, likened it to George Orwell's novel *1984. 1984* describes a dystopia, a dictatorship so powerful that there is no breaking free (Orwell, 2013). The book has many aspects, one of those being surveillance of citizens. In Orwell's book he describes them as 'Telescreens' - a two way mirror, into peoples living spaces. People are constantly watched to make sure they are not behaving in an unorthodox fashion - never questioning the state, or having independent thoughts. I feel that Lichtblau's technician was not wrong to think of Orwell in this instance. Secret rooms, in telecommunication companies offices, there to intercept communications. A feeling of being watched, concurrent with Orwell's dystopia. As I have already stated, *1984* had been my starting point with this research report, and now my initial suspicions about the sneaky, undercover actions of the NSA are shown to be correct.

This part of the report is written in the order of events happening - a timeline behind the NSA's surveillance operations, leaks, and the Snowden files. I compiled this together by using an activist website called Electronic Frontier Foundation (EFF) dedicated to revealing how surveillance in the modern age works, and where it has come from.

The Timeline

In 2003 and 2004, questions were raised by leading officials, all were either ignored or told they were wrong. For instance on the 17th of July 2003, Senator Rockefeller questioned the Vice President about the legality of the program. He never received a response. Likewise on March the 6th 2004, OLC head Goldsmith told the White House that they must cease some data collection (Inspector General Report, pg 462, 2009), but the White House disagreed. Only four days later when the Deputy Attorney General refused to sign another 45 day extension for the NSA program, the White House simply left the signature box blank, claiming it was still legal.

For me, questions about legality arise from this. If the Bush administration are able to implement, or authorise something without a critical signature (the Attorney General at the time was ill in hospital and unable to sign the authorisation, so his deputy had to), how is it possible to regulate what the President can do? Again, this question

about what is constitutional comes up, and again, the Bush administration squander it, and simply push through their own agenda, not giving a thought to the underpinning of American society. However, as it turned out, they were not free from scrutiny by the press.

Disaster struck for the Bush administration and the NSA in December 2005, when the New York Times revealed, in an article titled 'Bush Lets US Spy on Callers Without Courts', that the NSA had been spying on US domestic communications without warrants since the September 11 attacks. The New York Times said "…officials familiar with it [Stellar Wind Program] say the N.S.A. eavesdrops without warrants on up to 500 people in the United States at any given time." (Risen & Lichtblau, 2005). The officials in question had received anonymity due to the nature of the program. The same officials had felt uncomfortable with the legality of the program, as they told the New York Times: "…officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches." (Risen & Lichtblau, 2005).

With this out in the open, Bush had to respond to the allegations, and admitted the following day that the NSA had been eavesdropping on US communications with Afghanistan. Six days later the New York Times reported the same officials claiming the program had gone far further than what Bush had acknowledged. "The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said." (Risen & Lichtblau, 2005). They then claimed that to obtain this information the NSA had plugged into the very 'arteries' of American communications, meaning that they were tapping into far more than just US communications with Afghanistan.

It may have been a good idea, at this point, for the President to issue a full investigation into NSA surveillance, this may have won back some credibility. Not unsurprisingly, that didn't happen. The government was so involved with the surveillance the NSA carried out, that it would have been political suicide for Bush to do this. Instead, the information was brushed under the carpet. A government cover up, the next stage in the illegal, and extensive operation of NSA surveillance.

In June 2008 the FISA Amendments Act passed the House of Representatives. According to Republican Bobby Scott, the Act permitted the NSA to spy on all

communications entering and leaving the United States, irrespective of any wrongdoing from either party (Electronic Frontier Foundation, n.d.).

It became clear at this stage that the NSA, and the Bush administration, had been breaching protocol: broad scale surveillance of all domestic US communications, warrantless wiretapping of many US citizens without any evidence of wrongdoing taking place. A complete lack of cooperation from the Bush administration on where the program was heading, and a complete oversight of the legality of the program. From my perspective, Stellar Wind is a complete violation of the Fourth Amendment, and does not comply with the purpose of FISC. This is exactly the reason the special Court was formed in 1978, to watch over the NSA and make sure boundaries were not being crossed. And yet, the Court seemed powerless to prevent an Orwellian style surveillance system springing up after the September 11 attacks. There needed to be a change of government, a new leader, a new voice, a new Commander in Chief.

The election of President Barack Obama in 2009 began a new chapter in American history. Not only was he the first black President of the United States, he was also, to many people, a breath of fresh air in a stifling age of surveillance and war in the Middle East. He was the beginning of a new era - where the people forgotten by society would finally have a voice. Anything seemed possible at Obama's inauguration. However, the most startling revelations of state sponsored spying were to come about during his term as President.

Despite this, 2009 saw a clamp down on the extent of the NSA's reach. Firstly, on the 2nd of March, FISC ordered that the NSA must have court approval before carrying out metadata searches. This made sure that the NSA couldn't just search their own databases for communications without a court approval. Secondly, FISC forced, through a new court order, stating that the NSA must present to the court every instance where information was shared with other countries agencies. This was to be a weekly update on any intelligence sharing the NSA were involved in. Later, in 2009, FISC lifted this requirement. And thirdly, and I think, most importantly, an Inspector General Report was released to the public. This report was cowritten by the Justice Department, Defence Department, the Central Intelligence Agency (CIA), the NSA and the Office of the Director of National Intelligence. It outlined the program first enacted in 2001, and shed light on the NSA's handling of data. Glancing through the original report, however, shows that many areas of the report have been blacked out.

Censorship of declassified government material is common, but makes reading the report rather tricky as key aspects are missing. And censorship of this kind also hides from the public vital pieces of information. In other words, the really incriminating evidence is censored and will never be released. So how can the government be held to account? When the full picture is not released, it is impossible to make a full judgement of actions taken by the government.

According to an article by WIRED titled *'Watch What You Say'*, in January 2011, the NSA began construction of a massive new centre in Utah, allegedly costing the American taxpayer around $2 billion. The centre was heavily fortified against any intrusion, and inside, the NSA had giant rooms filled with data storage systems. The purpose of the centre was to farm US domestic communications. WIRED said the centre was to collect "…communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'" (Bamford, 2012). I think collection on this scale is beyond what can be claimed as 'counterterrorism'; it's beyond moral acceptability, it's intrusive. Intrusiveness and morality are at the forefront of the questions that should be considered when looking at the NSA's program, and I will look at this in greater detail on page 23.

WIRED reported an official, working for NSA, as saying "Everybody's a target; everybody with communication is a target." (Bamford, 2012). I am going to take a brief step back and ask, who were the original targets? The targets, according to Bush and his administration in the period right after 9/11, were the people plotting to attack the United States - the so-called terrorists. In the time since, one of two things has happened. Either, there was a switch, somewhere in the previous 10 years where the NSA, or the government, decided that looking for terrorists was no longer the priority, the priority then became collecting as much intelligence as possible, and anyone communicating became the target. Or, the darker alternative is that the plan was always to target ordinary communications, to collect and analyse information that wasn't just to do with counterterrorism. Maybe the program from the very beginning has always been to track ordinary people, and terrorism was just the excuse.

Edward J Snowden

In 2013, Edward Snowden's revelations shocked the world. Edward Snowden, an aspiring NSA contractor, turned whistleblower, leaked thousands of classified documents about the extent of the mass surveillance program the NSA were involved in, to the Guardian newspaper. Snowden now lives in Russia, hiding from the US government which has charged him with theft of government property and two accounts of violating the Espionage Act. Each account holds a maximum of ten years imprisonment in a federal prison, and a closed trial - meaning that Snowden could not make his case in front of a jury.

Edward Snowden first flew from Hawaii to Hong-Kong in May 2013, in a hotel room there, he chatted to Guardian journalist Ewen MacAskill. Since the documents released by Snowden hit the press, he has tried to gain asylum in many countries around the globe, such as Germany and Norway. It is likely that this plea will be granted, one day, as many of the documents that he released show the NSA's actions against those countries. The Guardian began releasing information about the documents on the 5th of June 2013. There were many victims to the Snowden files, not just the NSA, but GCHQ in the UK, companies that had collaborated to an enormous degree with surveillance programs, and other smaller security agencies around the world. After the Guardian began printing the documents, huge questions began to raised about the reach of the security agencies.

I feel that the press definitely have a role in society, sometimes they over-fill that role, but in this instance the Guardian was correct to highlight what the NSA were doing, and how that effected the public. Interestingly, David Cameron, the British Prime Minister at the time, warned the Guardian in advance not to publish any of the documents. The Guardian then published his advice which simply made him and the British government, look guilty. The press have a duty to identify and hold to account politicians and the government, in an ideal world, their primary role is to make sure the public is informed about what their government is doing. The Guardian, in this case, is simply informing the people of the UK and the world, about the covert operations of, particularly, the NSA and GCHQ.

From this moment on, I will be looking at the various operations exposed by Snowden, and the implications of those on society. This is where the timeline ends, and where the information that came to light in 2013, is presented.

Prism

The first of the leaks described a program called Prism operated by the NSA. Leaked slide shows of the program, which had been used to inform employees of the program at the NSA, show its purposes and potential. Prism was a collaboration between the NSA and communications companies, a collaboration far in excess of what was seen before. It allowed the NSA to tap into the very foundations of the companies and gain access to their customers data, either by obtaining stored data, or live data. For instance, a company like Skype, which was part of the program, could provide the NSA with a live feed of video streaming, or the NSA could obtain a Skype conversation that had already happened.

The companies involved in the program, and the order in which they joined, are as follows: Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL and Apple (Greenwald & MacAskill, 2013). According to the Guardian, when the newspaper reached out for a statement from these companies, they all denied knowledge of Prism. “An Apple spokesman said it had "never heard" of Prism.” (Greenwald & MacAskill, 2013). The response from Google was more cryptic, but still shied away from revealing a government connection to the company. “Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a back door for the government to access private user data.” (Greenwald & MacAskill, 2013). If the leaked documents are to be believed, which they should as they have been ratified by the Guardian, it is clear that to preserve their own customer support, both of these companies, and the others which claim to protect customer data, have blatantly lied about NSA involvement in their systems. The Guardian points out, rather ironically, a Microsoft slogan in use in 2013 which read: ‘Your Privacy is our priority’ (Greenwald & MacAskill, 2013). Microsoft were the first company to sign up to the NSA Prism program, as the documents show. However, as this slogan shows, this particular company, still has the audacity to lie to its customers, which gives the slogan an almost comedic edge.

Immunity was granted to the companies that complied with the NSA by Congress back in 2008. However, these companies could face legal battles in Europe or anywhere outside the United States. It is, perhaps, understandable that these companies deny the

claims relating to Prism as the NSA most likely placed a lot of legal pressure on them to comply. However, they should still be accountable to their customers. Accountability is another theme that is well worth exploring. Who is accountable anymore? The government, through censorship, lying, and blatant disregard for constitution, appears unaccountable to its own citizens. Aided, nevertheless, by companies. Companies that should be fully accountable for their actions to paying customers and shareholders. However, we see here, that neither the government, or the companies are accountable for their actions. They simply deny it.

The access granted to the NSA by the companies was profound. "The Prism program allows the NSA, the world's largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders." (Greenwald & MacAskill, 2013). Due to court orders in 2008, the NSA do not even need to prove that one of the participants in a single communication is outside the United States, as the order states that there only needs to be a 'reasonable' belief of either the sender or receiver being outside the United States. This leaves the NSA in a position where they can pretty much legally listen in to any communication they choose that goes via one of these companies.

A leaked presentation slide by Snowden (on the following page), shows a computer program that colour codes the amount of information obtained from any given country, to help provide the NSA with a clear description of where their intelligence is coming from.

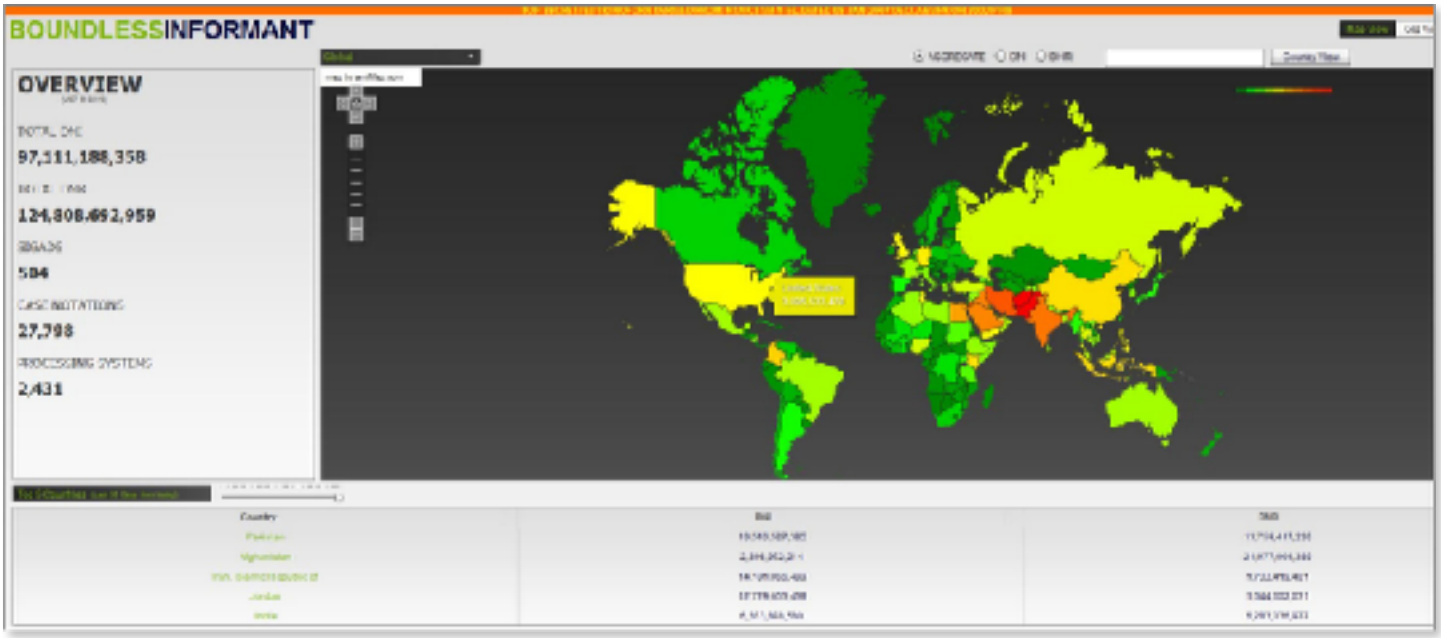


Figure 1 - Boundless Informant (Greenwald & MacAskill, 2013)

The software was called 'Boundless Informant', and provided any NSA official immediate visual clarity about how much information was being gathered, and from where. The software comprises both internet communication records (DNI) and telephone communication records (DNR). From my perspective, the numbers are largely meaningless, as there is no comparative information for me to work with, however, what this slide shows, using colour coding, is the amount of information gathered in countries comparative to each other. The colour coding goes from dark green, being a small amount of information, to dark red, being a lot of information. Taking this into account it is easy to see that the NSA collects far less information from Canada than it does from Afghanistan. This is expected, however, as the US government says that is where the enemies of the US are. The more interesting aspect of this slide shows that more information is being gathered from the United States, or the UK, or Germany, than from Russia, or Kazakstan, or even many large African countries.

I return again to the question, who are the targets? If one considers this to be a map of where potential targets are, which is sensible as the Middle East is heavily coloured red and where the enemies of the United States are located, potential targets, judging by the amount of information collected from each country, are to be found in great abundance in the UK, US, and Germany. One thing the numbers do tell us, is

that the amount of information gathered is large, therefore it can be assumed that the information gathered is far in excess of just a few Jihadi leaning targets who might qualify for counterterrorism surveillance. Drawing conclusions from this, it is unclear what the true aim of the NSA is.

It is becoming obvious that as counterterrorism surveillance increases, the privacy of ordinary citizens decreases.

Tempora

The Snowden files showed that mass surveillance wasn't just a cancer inflicted by the NSA. The files showed a heavy involvement of GCHQ in mass surveillance, the UK equivalent to the NSA. It had been clear for some time that GCHQ was the little brother to the NSA, and, at times, the NSA been critical about the amount of intelligence GCHQ had contributed too. NSA officials have been known to have said that GCHQ needs to pull its weight in its information gathering. "In one revealing document from 2010, GCHQ acknowledged that the US had 'raised a number of issues with regards to meeting NSA's minimum expectations'. It said GCHQ 'still remains short of the full NSA ask'." (Borger & Hopkins, 2013). The Snowden files revealed that GCHQ had responded to this by tapping into global fibre-optic cables carrying information around the world. In 2011, they set themselves a summer project - to intercept 200 fibre-optic cables that run underneath the Atlantic, surface for a short while in the UK and then go to the European continent. The cables carry things from phones calls and conversations, to FaceBook statuses. By 2012, the files show, GCHQ had achieved their goal. 21 petabytes of data every day (according to the Guardian this is "…equivalent to sending all the information in all the books in the British Library 192 times every 24 hours." (MacAskill & Borger, 2013)), could now be intercepted by GCHQ. The digital world of any person around the globe was now open for inspection by GCHQ. The program was codenamed 'Tempora'. Tempora represents a huge threat to the privacy of ordinary citizens around the world. The Guardian states: "For the 2 billion users of the world wide web, Tempora represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world." (MacAskill & Borger, 2013). The intrusiveness of this level of intelligence gathering is can be seen as a war on global privacy. The Snowden files show that GCHQ were focused on developing faster super-cables in order to intercept and analyse

more data. All this intelligence was immediately shared with the NSA. The collaboration of these two security agencies poses questions about what happens to the data collected and how much of it is sifted and analysed. Further collaboration became apparent as more revelations from the files were revealed by Snowden. Allegedly the NSA paid GCHQ 100 million pounds in order to influence who GCHQ spied on, and how much data they shared with the NSA. In exchange, GCHQ had access to the whole of the NSA's vast database on all communications globally.

It is clear that at the time of the files being released, the NSA and GCHQ were highly intertwined, and worked together on mass intelligence gathering. These two agencies also worked closely with three other countries' intelligence agencies in an alliance called The Five Eyes Electronic Alliance, commonly abbreviated to Five Eyes or FVEY. The alliance was an intelligence sharing platform made up of the countries Australia, Canada, New Zealand, the United Kingdom and the United States. Common ground and law systems enabled the five countries to work in unison, collecting signals intelligence (SIGINT) from around the globe. Just like any alliance, there are players that contribute more than others. The main players in FVEY, were GCHQ and the NSA, and both had substantial budgets from their respective countries governments.

Treasure Map

In 2013 two newspapers, Der Spiegel and The Intercept, both began printing reports on the reach of Fives Eyes. The files show that the NSA and GCHQ, were doing far more than just picking up communications between two people, they were also beginning to map locations and communications from every single device with an electronic signal. These two leading security agencies had hacked and negotiated access into satellite companies gaining entry to location specific data and communications. The Intercept said: "It evokes a kind of Google Earth for global data traffic, a bird's eye view of the planet's digital arteries." (Müller-Maguhn & Poitras et al, 2014). A global map of what's happening where and at any time. Any device, in this day and age, is connected somehow to the internet. Internet servers providing that signal usually go via a satellite, the satellite then determines the real time location of the device using the server. GPS (Global Positioning System) is usually accurate to within a few metres, and so GCHQ and the NSA can gain access to the information that a device is receiving

and sending, it gives the agency a full picture of what is going on there at that particular instant. This is a global operation, and enables GCHQ and the NSA to have, as The Intercept stated, a Google Earth type software, but with data and information, instead of satellite images. This program was codenamed 'Treasure Map'.

With locations and communications both going through these agencies, it enabled them to pick a certain person and create a 'character profile'. Now, I'm not suggesting that the NSA and GCHQ were watching and creating a profile of everyone, as they would not have the resources. However, this program enables them to create a profile on anyone they choose. For example, they may not have watched every single person in Germany, but they can watch any individual if they find a reason. Profiles are built up using information about what that person does and who they talk too. For instance, with location tracking, the NSA could find out any person's place of work, and how long their shift is, and who else they were with. From their communications they could find out who that person talks too, or what that person searches on the internet. Online purchases, browsing, YouTube videos, text messaging, FaceBook activity, friends and family. After a little amount of time the agency could have known that person intimately and then decide whether they were a threat.

Treasure Map is a golden jewel for a security agency wishing to exercise maximum power. The authority, and power that being able to tap into anybody's phone and find out where they were, and what they were doing at any given time, provides a very superior feeling. Being able to control diplomatic negotiations by how much intelligence is gathered, being able to identify someone wherever they go, or tracking a supposed terrorist gives an agency a feeling of supremacy, of living above everyone else, of living - perhaps, above the law. This is another, more subtle, piece of evidence that shows how the security agencies operate outside, and in violation of, the constitution. The feeling of watching over a population, sets them above that population. And once that has been established, it allows said agencies, to operate as if they are, in fact, above the law.

All the intelligence collected from around the globe was too much to analyse at once, so agencies stored and gathered information so that it is possible to go back and analyse events after they have happened. The approach taken by the agencies was, in order to, track, monitor and survey tomorrow's target, the agencies would require today's intelligence.

Conclusion

There is a definite moral question behind surveillance of this kind. Is it right to sacrifice privacy in exchange for protection? This is tricky as it is subjective. By that, I mean, morality is opinion based, and so is different for each person. The security agencies take the line: 'You have nothing fear, if you have nothing to hide.' Personally, I morally object to have my phone tapped or communications intercepted, not because I'm a terrorist, or a murder, or an enemy of the state, but because I require privacy in order to operate as a human being. If a communication of mine is intercepted, which is perhaps inevitable, I don't know who is viewing it or how it is being used. Communication sharing between the British and the Americans was at an all time high when the Snowden files were released. GCHQ and the NSA worked very closely on intelligence gathering and viewing, and so a foreign government could be viewing what my communications were. Who I was talking too, when I was talking to them, my GPS location, all of this could have been shared with the United States. I could become a potential target, just because I communicate.

Maybe part of the problem is that there is no transparency or accountability. The public don't know what these agencies are doing supposedly with the public interest in mind. GCHQ and the NSA are just secret agencies, doing secret things with our data, and regulated by courts without backbone all in the name of counterterrorism. It is only then, leaks from morally guided rare heroes like Edward Snowden that show us what is really going on.

And after learning so much about what our security agencies are doing, the obvious question remaining is: does it work? In order to answer this, I return to what the NSA's program was originally set up to do, or claimed to prevent. In wake of the September 11 attacks George W. Bush declared the War on Terror, a war not just of military action in the Middle East, but a war waged with the help of a new kind of technology. In order to foil terror attacks before they even happened, George W. Bush signed the President's Surveillance Program. As I have already stated, the program enabled the NSA to collect massive amounts of data, in order to catch the few that were planning terror attacks. Or so it said. The pure scale of the program became apparent with the Snowden leaks, and subsequent leaks by WikiLeaks. Considering all of this, we have to ask ourselves what we expect from this type of surveillance. And therein lies the problem with working out whether it is working or not. In short, if the expectation is

that there should be no terror attacks with this type of surveillance, an opinion that helped Bush pass the program in the first place, then the program has failed.

The Bataclan terror attacks in Paris in 2015 support this statement, as did every other terror attack that has happened since 9/11 (such as the 7/7 bombings in London in 2005). Within months of the atrocities in Paris taking place, it became apparent that the security agencies knew about the terrorists in advance, the people committing the atrocities were on a special watchlist - as were many many other people. And that's the problem, observing the whole haystack, does not guarantee finding the needle. If the watchlist extends to say 30% of the population, how can the NSA ever hope to find the few enemies of the state?

In fact, although it may be controversial to say it, the NSA appear to benefit from terrorist attacks. The NSA gained massive power after the attacks on September 11 2001, they were entrusted with the security of United States. Its paradoxical. If no terrorist attacks happen, how do the population know that there is still a true threat to them and their society? It seems that, only with terrorist attacks, do agencies, such as the NSA, have the necessary political and public support to do their job. It could be, therefore, beneficial for them for a few terrorist attacks to be 'allowed' to happen. I understand that is a serious allegation to make, and I say it in a purely hypothetical sense. I am not suggesting that the NSA, GCHQ or any security agency allows terror attacks to happen to benefit their own interests. I am merely stating that they appear to benefit from atrocities, such as 9/11, taking place. For instance, French security agencies, undoubtedly, benefitted from an increased governmental support after the Paris attacks in 2015. The attacks reminded people and the French government of the threat of terrorism, it reminded people that the security agencies are needed. A fine balance is needed then, where enough terror attacks are thwarted and enough are let through in order to keep the public opinion, and government support, on side. If this were the case, security agencies have their own agenda, and their role is no longer to protect the public, but to protect their own continuation.

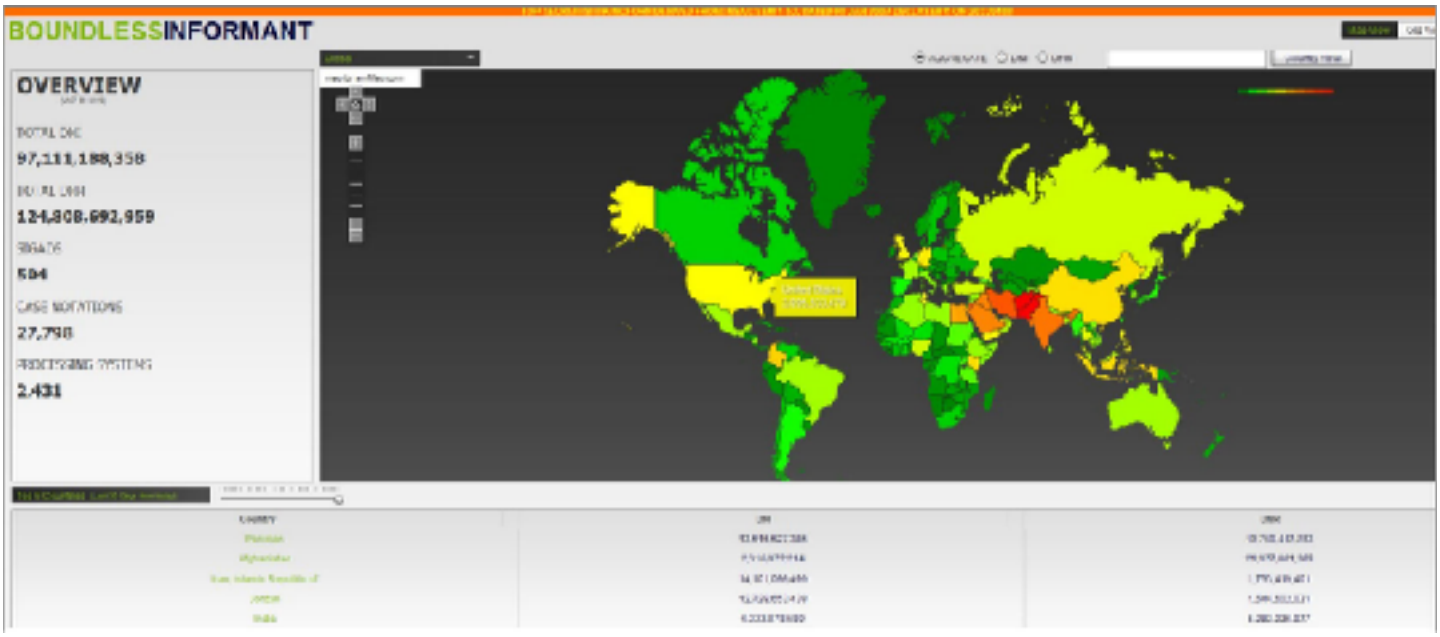
Through the process of writing this research report, I have come across things that have shocked me, such as Treasure Map, or the violation of the US legal system; and things that I expected to find. For instance, I already thought that the NSA and security

agencies alike, benefit from terror attacks. I also, having seen *Fahrenheit 9/11* in the past, expected to find dodgy, secretive actions initiated by the Bush administration.

My research has shown me the answer to a few of the questions stated in the introduction to this report. However, a couple of them, I have found, aren't entirely answerable. For instance, the accountability of governments. The US government, in my eyes, has breached the American constitution. However, I fail to see how it is possible to hold the government to account if the government doesn't tell the public or the press what they are doing. How is it possible to monitor one's own government, if its information is classified and kept completely secret? And if the government doesn't want anyone to know, they will never declassify it. We are simply asked to place our trust in politicians and governments, and hope that they find some moral respectability about what is right, and what is clearly wrong. The Snowden files showed us that politicians cannot see the this distinction. Their own agenda corrupts their decisions, and distorts any kind of line that should never be crossed.

Throughout this report I have tried to delve into the very depths of what is happening with our security agencies, what they are doing, and why, they say, they are doing it. However, I come to the conclusion that it is not the agencies that are the problem, it's the governments that authorise their behaviour, and the oversight of legal obligation. The scale of what is happening is extraordinary, and it's all happening behind closed doors. Surely, this isn't the kind of world envisaged in 1776, with the American Declaration of Independence?

Figure 1 - Boundless Informant (Greenwald & MacAskill, 2013)



References:

1. Ali, S.S.A & Abdullah, H.A. (2016). *Did the Patriot Act Change US Attitudes on Surveillance?* Retrieved 10 May, 2017, from http://www.nbcnews.com/storyline/9-11-anniversary/did-patriot-act-change-us-attitudes-surveillance-n641586
2. Arnold, C.A. (2007). *'It is Their Right, It is Their Duty, To Throw Off Such Government'.* Retrieved 10 May, 2017, from https://www.commondreams.org/views/2007/07/01/it-their-right-it-their-duty-throw-such-government
3. Bamford, J.B. (2012). *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say).* Retrieved 10 May, 2017, from https://www.wired.com/2012/03/ff_nsadatacenter/
4. Borger, J.B. & Hopkins, N.H. (2013). *NSA pays £100m in secret funding for GCHQ.* Retrieved 10 May, 2017, from https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden
5. Butler, T.B. (n.d). *The Media Construction of Terrorism Pre and Post-9/11.* Retrieved 10 May, 2017, from https://www.mckendree.edu/academics/scholars/butler-issue-24.pdf
6. Cauley, L.C. & Diamond, J.D. (2006). *Telecoms let NSA spy on calls.* Retrieved 10 May, 2017, from http://usatoday30.usatoday.com/news/washington/2006-02-05-nsa-telecoms_x.htm
7. Electronic Frontier Foundation (n.d). *Timeline of NSA Domestic Spying*. Retrieved 10 May, 2017, from https://www.eff.org/nsa-spying/timeline
8. Gallagher, R.G. (2013). *NSA Even Spied on Google Maps Searches, Documents Suggest.* Retrieved 10 May, 2017, from http://www.slate.com/blogs/future_tense/2013/07/11/xkeyscore_program_may_have_allowed_nsa_to_spy_on_google_maps_searches.html
9. Greenwald, G.G. & MacAskill, E.M. (2013). *Boundless Informant: the NSA's secret tool to track global surveillance data.* Retrieved 10 May, 2017, from https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
10. Greenwald, G.G. & MacAskill, E.M. (2013). *NSA Prism program taps in to user data of Apple, Google and others.* Retrieved 10 May, 2017, from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

11. Heiligenstein, M.X.H. (2014). *A Brief History of the NSA: From 1917 to 2014.* Retrieved 10 May, 2017, from http://www.saturdayeveningpost.com/2014/04/17/culture/politics/a-brief-history-of-the-nsa.html
12. History.com Staff (2009). *Watergate Scandal.* Retrieved 10 May, 2017, from http://www.history.com/topics/watergate
13. Inspector General Report (2009). *Report on the Presidents Surveillance Program.* Retrieved 10 May, 2017, from https://www.documentcloud.org/documents/2067784-savage-foia-stellarwind-ig-report.html#document/p12
14. Legal Information Institute (n.d). *Fourth Amendment.* Retrieved 10 May, 2017, from https://www.law.cornell.edu/wex/fourth_amendment
15. MacAskill, E.M. & Borger, J.B. & Hopkins, N.H. & Davies, N.D. & Ball, J.B. (2013). *GCHQ taps fibre-optic cables for secret access to world's communications.* Retrieved 10 May, 2017, from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
16. MacAskill, E.M. & Dance, G.D. (2013). *NSA files decoded: Edward Snowden's surveillance revelations explained.* Retrieved 10 May, 2017, from: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
17. Müller-Maguhn, A.M.M, & Poitras, L.P. & Rosenbach, M.R. & Sontheimer, M.S. & Grothoff, C.G. (2014). *The NSA and GCHQ Campaign against German Satellite Companies.* Retrieved 10 May, 2017, from https://theintercept.com/2014/09/14/nsa-stellar/
18. Orwell, G.O. (2013). *1984.* (1st ed.). Great Britain: Penguin Books.
19. Peterson, D.P. (n.d). *The Patriot Act & Title II Surveillance Procedures.* Retrieved 10 May, 2017, from http://www.apexcctv.com/Articles/patriot-act-title-II-surveillance-procedures.html
20. Risen, J.R. & Lichtblau, E.L. (2005). *Bush Lets U.S. Spy on Callers Without Courts.* Retrieved 10 May, 2017, from http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html
21. Vargo, S.V. (2015). *There's nothing patriotic about the PATRIOT Act, and there is no proof it's even working.* Retrieved 10 May, 2017, from https://www.opednews.com/articles/2/There-s-nothing-patriotic-by-Samuel-Vargo-Advisors_Drone_Government_Obama-150531-990.html