Leeds Beckett University
Faculty of Arts, Environment & Technology

MSc Business Intelligence

Academic Year 2015-2016

Joanne Kennedy C3369865

MIDGE Academic Report:

The boundaries of privacy and data protection will be redefined

Date of Submission: 12th January 2016

Contents

Article I. Introduction

The private and public sector are constantly expanding their data sets as we live in the digital and information age. Many people share their personal data through the phenomena that is social media, along with this and online activity tracking systems; it is easy for companies to gather data and intelligence on individuals. (IFLA, 2015)

Government agencies find it beneficial to collect large amounts of data in order to aid their advanced profiling techniques when looking at criminals and suspects. The use of monitoring and filtering the collected communication data will consequently result in allowing the tracking of these criminals and suspects to be made easier, providing a more time and cost effective solution to crime detection and prevention. (IFLA, 2015)

Tracking online activity and filtering the data is undertaken with the use of mass monitoring of the communication data and metadata from devices and platforms, certain advances in technology have made this much easier and cheaper, and it will continue to do so. (IFLA, 2015)

Devices themselves aid investigations for example mobile phones have the well known GPS trackers inside them, although this can be switched off and the data file containing the locations can be manipulated, what many people don t know is that most smartphones also now come with a motion tracking chip inside, in order to detect movement. This feature can then be used to identify previous locations that have been visited and even re-construct a crime scene. (CSI Cyber, 2015)

Along with cookies and mouse-click tracing, companies are using emotional metering with the use of social media and retina-movement analysis to improve sophistication which can be a great way to promote certain products and therefore generate more sales. Unfortunately the access to personal data has provided companies and organizations the capability of deploying discriminatory pricing and this is why many companies have begun to advertise privacy on their websites, in

order to let users know they are protected, which is a positive way to build trust between a company and its consumers. (Rudasill, 2014)

Government agencies are putting intense pressure on companies to provide them with their collected communication data, associated metadata and online activity records in order to build on their datasets. However this has caused some controversy amongst the public as this is private and personal data that is being passed around without the need for consent. (IFLA, 2015)

If governments were to use algorithms resulting from user s previous internet searches and past purchase history, similar to what companies such as Amazon use to monitor their customers, it could easily provide a false assumption about someone. (Rudasill, 2014)

Article II.

Section 2.01 A Surveillance Society

Surveillance is becoming essential in everyday life and in everyday environments in order to maintain public safety. For years now everyone has been aware that CCTV cameras operate in public areas such as shops, roads and train stations. However CCTV in the workplace and in schools is ever-increasing. But is the obsession with CCTV becoming more of a novelty than a benefit?

There are many mixed feelings on surveillance cameras in schools and a study shows that the majority of teachers were initially paranoid about the installation of CCTV, however the presence of the cameras was soon forgotten about and not many teachers could describe the exact location of the cameras. On the other hand students were very clued up on the camera locations and could even report where there was no camera coverage, which was very worrying. (Taylor, 2011)

In some schools they have made sure that there are no blind spots, and they even have CCTV cameras in student toilets and changing rooms, however this could be classed as a clear breach of privacy and in situations like this it is understandable why students and parents do not agree with surveillance in schools. (Harris, 2011)

Who is monitoring these cameras? Just because someone has a clean record does not mean they are not criminals, they may have not yet been caught, or they may have not yet committed a crime, but it doesn t mean they won t in the future. Another question to ask would be where is the footage been stored and how long is it stored for? In a study a teacher stated I certainly wouldn t expect them to be put in the staff toilets. So shouldn t the students be given the same respect? (Taylor, 2011)

Bullying, behaviour and crime are problems schools have to tackle on a daily basis and improving these matters is a priority for the government. CCTV cameras can provide a safety measure for victims that are being bullied, and a surveillance measure to monitor behaviour. (Harris, 2011) CCTV can also be used to settle any claims that may arise against staff and capture the presence of any intruders in or around the school grounds. (Taylor, 2011)

Cyber bulling is constantly on the rise due to the advances in technology and schools try to do as much as they can to help protect against this crime. Although CCTV may not aid in lowering cyber bullying, new laws give schools surveillance authority over student s online and electronic activity. (Suski, 2014)

Surveillance cameras in the workplace can be used to prevent crime such as theft and violence, it can be used to ensure health and safety rules are being adhered to, it can prevent misconduct, improve productivity and ensure legal and regulatory obligations are being complied with. However there are three main risks that companies need to take into account, the first being the maintenance of trust and confidence as this can easily be lost between companies and their employees. (Sinclair and Annereau, 2014)

The second risk to bear in mind is the Data Protection Act 1998 as a breach of this could result in sanctions and bad publicity for the organisation. It could also result in a Subject Access Request which is becoming increasingly popular due to employees wanting disclosure on the data and footage held about them. The third risk to consider is the Human Rights Act 1998 which is in place to ensure the monitoring taking place is not intrusive. (Sinclair and Annereau, 2014)

Once trust has been lost in a workplace it is very difficult to re-build and if CCTV is installed appropriately and used for covert purposes it seems very few people have a problem with this, however employees, like students believe certain physical boundaries within the work place such as toilets and changing rooms should be respected. (Agustina and Coudert, 2013)

Section 2.02 The Risks to Consider

When looking at mass surveillance and data collection it is important to consider all the risks this may have on society, and companies must ensure they take into account ethical considerations.

Data privacy is one of the main risk factors when collecting big data and a risk mitigation strategy is essential to ensure the data remains secure. Privacy risks can be divided into four main categories; information collection, information processing, information dissemination and invasion. (Polonetsky et al, 2014)

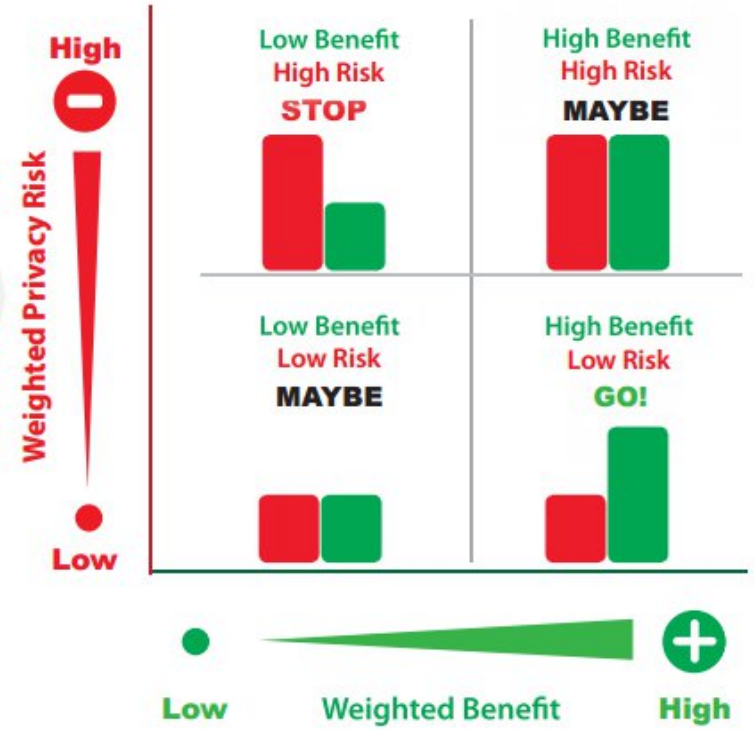

Figure 1: Data Benefit-Risk Analysis: STOP or GO? (Polonetsky, 2014)

The government has many secret surveillance projects and not only does the government want to ensure these projects stay secret but, they also want to ensure the mass data that is being collected remains secure. In the past there have been a number of leaks within the government and this is why it is important to consider the implications that would arise if the data was to be leaked to the public.

When the public first became aware the government was using technology to provide mass surveillance it was considered a clear breach of civil liberties. The Human Rights Act 1998 states everyone has the right to respect for private and family life without the intrusion of public authority, yet there is an acceptance clause which states if it is deemed necessary in order to prevent crime, and aid in the well-being of the country this act can be breached. (Wikipedia, 2015)

In February 2015 Government Communications Headquarters did breach the Human Rights Act 1998 by accessing data from the National Security Administration, although it is not known which companies had their data unlawfully shared. The human rights organisation Privacy International created a website which aided citizens in making claims of unlawful surveillance with the investigatory powers tribunal. (Human Rights Watch, 2015)

Legal standards are unable to deal with the current surveillance environment; the government have the ability to infiltrate networks and systems, monitor phones and computers and modify data without leaving a digital fingerprint. (EPRS, 2015) Although the public are forever losing their trust and confidence in government agencies, ending surveillance programs is not an option that would be taken unless the risk of terrorism significantly deteriorates. (Lewis, 2014)

It is important to consider the way in which the collection of data has changed the community over the given years. People are now known as a number in a database, rather than an actual person and if the data was to be shared with employers, companies and universities; this could portray a false impression of a person. People should not be defined by what they have done in their past, what companies they are or have previously been involved with, and what they communicate over the web and the telephone. (Preez, 2015)

Big data and mass surveillance can create inequality between the people being watched and the people that are watching, and this leads to the risk of blackmail, discrimination and coercion significantly increasing. (Richards, 2013)

When government files were leaked to the media in 2013, it was exposed that Government Communications Headquarters and the National Security Administration had hacked into Gemalto, which is the words largest SIM card manufacturer in order to steal encryption keys. (Privacy International, 2015)

Having access to encryption keys would allow agents to unlock mobile communications and intercept them, without leaving a trace and without requiring a warrant or even confirmation from telecom companies. (Privacy International, 2015)

It is vital that communication privacy is managed accurately; privacy boundaries are altered throughout a person s life-span in order to accommodate their needs. As seen below in figure 2, privacy boundary is at its largest during adulthood whereas during childhood, privacy is reduced due to safety matters and the fact that children are reliant upon someone else to fully accommodate their needs. (Petronio, 2002)

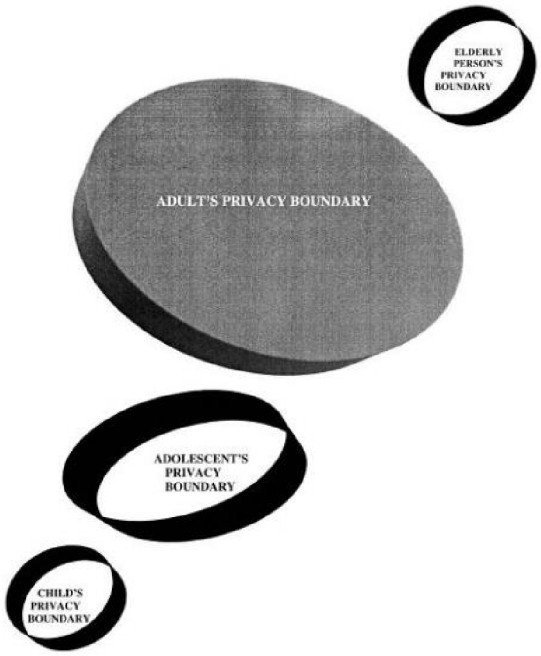

Figure 2: Boundary Life-Span Changes (Petronio, 2002)

Section 2.03 Government Libraries and Data

Data can be used to achieve the 17 sustainable goals which are to end poverty, end hunger, promote well being, quality education, gender equality, water and sanitation for all, affordable and sustainable energy, decent work for all, technology to benefit all, reduce inequality, provide safe cities and communities, promote responsible consumption by all, stop climate change, protect the ocean, take care of the earth, live in peace and provide mechanisms and partnerships to meet the goals. The trend is moving towards open data which will acknowledge the public s right to access information, however it is important to respect privacy and manage the information overload, and this can be done with the use of certain laws, legislations, policies and practices. (Hamilton, 2015)

In order to comply with these laws, legislations, policies and practises, thirteen principles have been created that must be followed.

- The first principle is legality which means any constraint which may affect human rights must be approved by law.
- The second principle is legitimate aim which only permits surveillance to take place when there is a legal interest and it is necessary in a democratic society.
- The third principle is necessity which means there is a legitimate aim behind, why surveillance is required.
- The forth principle is adequacy which means authorisation by law must be appropriate to accomplish the legitimate aim.
- The fifth principle is proportionality which means the sensitivity of the data collected and the infringement it would have on human rights must be fully considered.
- The sixth principle is competent judicial authority which means the judicial authority must be impartial and independent to the authorities conducting the surveillance.
- The seventh principle is due process which means human rights are respected and procedures are available to the public, enumerated in law and consistently practiced.

- The eighth principle is user notification which means those that are being captured on surveillance are notified about it.
- The ninth principle is transparency which means information should be provided which states the scope, nature and application of the laws permitting the surveillance.
- The tenth principle is public oversight which means oversight mechanisms should be in place to ensure transparency and accountability for the surveillance.
- The eleventh principle is integrity of communications and systems which ensure the security of the collected data and surveillance.
- The twelfth principle is safeguards for international cooperation which comes in to play when assistance from Foreign Service providers is required.
- The final principle is safeguards against illegitimate access and right to effective remedy which provides criminal penalties, protection and avenues for redress. (Necessaryandproportionate, 2014)

The main purpose of government libraries is to provide elected representatives, ministers, administrators, scientists, researchers and the general public access to data and information written by government and non-government individuals. Dissemination of information through digitization can help with both access and preservation. (Bolt and Burge, 2008)

No matter whom the user is it is vital to ensure the privacy of the use of government library resources remains intact and libraries must ensure they follow the laws of their own country to do this. It is especially important with the use of government information due to the greater opportunities they have when it comes to finding out what people are researching in their libraries. (Bolt and Burge, 2008)

Due to digital literacy progressively becoming important in society it is imperative that library users know that their digital footprint may be available to commercial and government agencies. This is why strategic privacy plans are in place to try and protect intrusions. (Rudasill, 2014)

In order to protect the privacy of users in libraries the national government policy on privacy of library use must be adhered to. The library should also create its own policy regarding privacy, and it should deploy privacy procedures for staff to abide. (Bolt and Burge, 2008)

It is also important to train the staff on the reasonings behind these policies and procedures in order to give them a greater insight into why retaining privacy is such an important factor within the organisation and ensure that they do not reveal information about library users at the request of the government or on their own accord. If a legal request was received it is important that staff are trained on how to handle this matter, in terms of knowing who has the authority to respond to such request and therefore who the request should be passed on to. (Bolt and Burge, 2008)

Another possible step in protecting privacy would be to remove records which link individuals to government resources once the resources have been returned and are no longer in use. However in some countries where freedom of information and respect for human rights policies are not in place this may not be legal so it is important to check you are still abiding by the law. (Bolt and Burge, 2008)

It is common for libraries to not allow photography to take place inside without written consent; however with the growing use of wearable technology such as google glasses, it is giving individuals opportunities to break this policy with the use of discrete and innovative technological products which may prove to be a cause for concern in the future. (Rudasill, 2014)

Section 2.04 Intelligence behind PRISM

PRISM is a secret surveillance program that became public knowledge when intelligence officer Edward Snowden leaked the classified information to the news. It was initiated by the US government in order to help the National Security Agency and the FBI to capture private data including metadata and content on citizens, and not just the citizens who are known criminals and suspects. (Sottek and Kopstein, 2013)

The government claim that data is only collected on specific targets and under a court approval, however the Foreign Intelligence Surveillance Court which was approved by the Foreign Intelligence Surveillance Act operates in secret, leading to members of the public wondering whether the program is violating their human rights. (Sottek and Kopstein, 2013)

The NSA use telecommunications and internet companies to gather their data by installing a fibre optic splitter switch which is used on the incoming traffic lines in order to send the traffic to an intercept station for processing; an example of this can be seen in figure 3. The NSA also builds back doors into software, provides secret court orders to companies and gains access to encryption keys. (Domestic Surveillance Directorate, 2015)

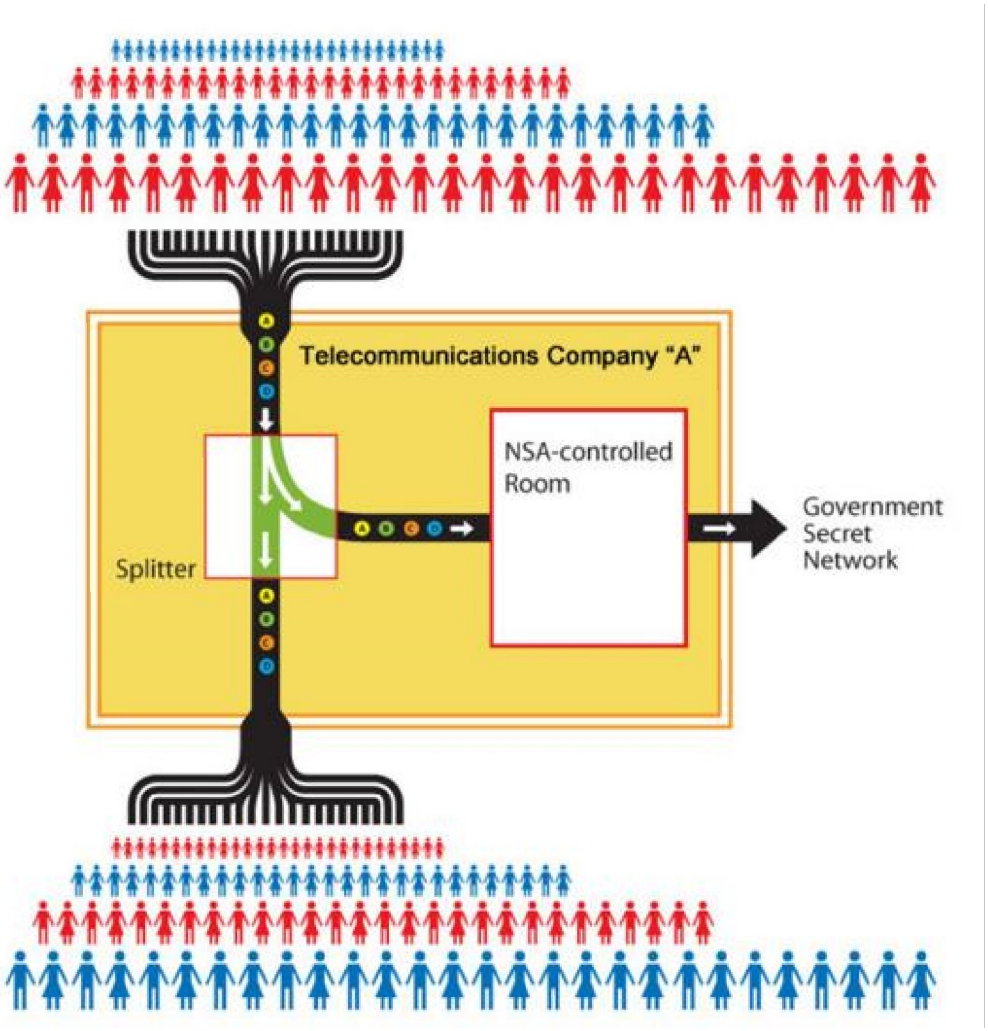

Figure 3: Intercepting Communications (Domestic Surveillance Directorate, 2015)

It has come to light that the government are using connections they have with major technology organisations that are greatly trusted in the online community such as Microsoft and Google amongst many others, a court order that was leaked revealed Verizon handed over all call records and metadata to the National Security Agency on a daily basis. (Sottek and Kopstein, 2013)

PRISM uses search terms to gather raw intelligence which is pulled from collections known as Signals Intelligence Activity Designators, only experienced intelligence officers and analysts are thought to be granted access to this program. (Sottek and Kopstein, 2013) The way in which data is gathered can be seen in figure 4 below.

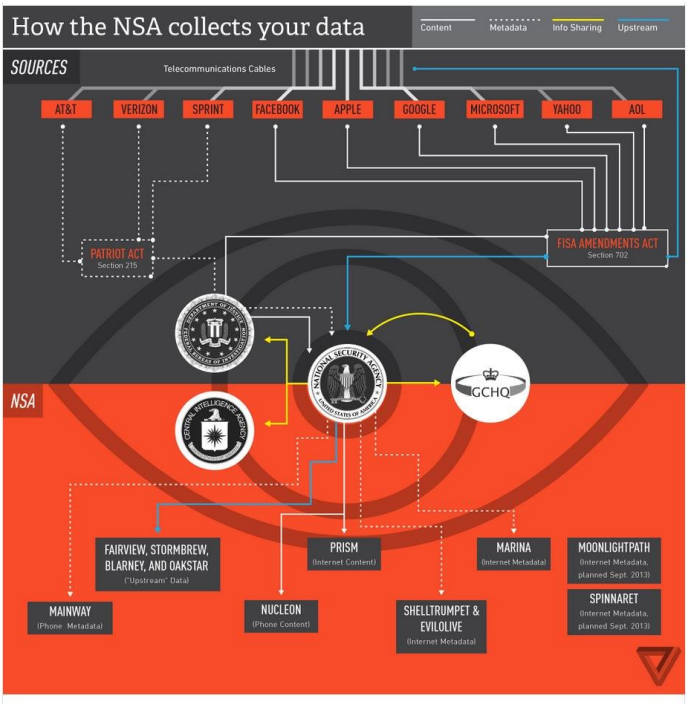

Figure 4: How the NSA collects your data (Sottek and Kopstein, 2013)

Article III. Conclusion

Although in the near future individual privacy and trust could be exploited, the benefits not only to the government, but to companies, workplaces, schools and the public in general much out way the risks and society probably could not survive without access to the required information and data.

The most important thing is to know the risks of over-sharing personal data on the internet as once a permanent digital footprint is left, it cannot be retrieved. Governments and organisations as discussed above monitor and filter data for their own benefit and sometimes this can lead to laws and legislations that are there to protect user s personal data, being bent and broken.

It is also important to consider that with new technological advances, comes a new breed of criminals and people posting photos of what their houses look like, including their locks and where they leave their keys can be potentially very dangerous. If the photos are geotagged anybody with Google Street View can view their house online and a survey of ex-burglars discovered that 80% of them used social media in order to find victims houses. (Troy: Cyber Hijack, 2015)

Due to mass surveillance technology becoming cheaper and more powerful, it is likely that in the future it will become more widespread, resulting in it becoming available to most countries. However different countries have different laws and legislations and some countries do not have a policy in place to protect user s privacy or rights, so this could lead to further problems. (Amnesty International, 2015)

Article IV. Bibliography

Agustina, J.R and Coudert, F (2013) **Limits and challenges of the expanding use of covert CCTV in the workplace in Spain beyond jurisprudential analysis**. [Online] Available from: <http://eds.a.ebscohost.com.ezproxy.leedsbeckett.ac.uk/eds/pdfviewer/pdfviewer?sid=4c3510f2-6857-4a80-be25-f93aecb61856%40sessionmgr4003&vid=1&hid=4102> [Accessed 27th November 2015].

Amnesty International (2015) **Two years after Snowden governments resist to end mass surveillance**. [Online] Available from: < https://www.amnesty.org/en/press-releases/2015/06/two-years-after-snowden/> [Accessed 16th December 2015].

Bolt, N and Burge, S (2008) eds. **Guidelines for Libraries of Government Departments**. International Federation of Library Associations and Institutions: IFLA Professional Reports. No.106. [Online] Available from: <http://files.eric.ed.gov/fulltext/ED510085.pdf> [Accessed 15th December 2015].

CSI Cyber, series 1 (2015) **CSI Cyber: The Evil Twin**. London: Channel 5, 3 Nov, 22:00.

Domestic Surveillance Directorate (2015) **Surveillance Techniques: How Your Date Becomes Our Data**. [Online] Available from: <https://nsa.gov1.info/surveillance/> [Accessed 16th December 2015].

EPRS (2015) Science and Technology Options Assessment: **Mass Surveillance**: Part 1: Risks and opportunities raised by the current generation of network services and applications. [Online] Available from: <http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf > [Accessed 23rd November 2015].

Hamilton, S (2015) **Libraries, development and the bigger picture: what will the post-2015 information environment look like for libraries?** [Online] Available from: <https://dayone.me/1We3zxh> [Accessed 27th November 2015].

Harris, J (2011) **School surveillance: how big brother spies on pupils**. [Online] Available from: <http://www.theguardian.com/uk/2011/jun/09/schools-surveillance-spying-on-pupils> [Accessed 27th November 2015].

Human Rights Watch (2015) **UK: Human Rights Watch Challenges Surveillance**. [Online] Available from: < https://www.hrw.org/news/2015/09/14/uk-human-rights-watch-challenges-surveillance > [Accessed 23rd November 2015].

IFLA (2015) **Riding the Waves or Caught in the Tide?** [Online]. Available from: <http://trends.ifla.org/files/trends/assets/insights-from-the-ifla-trend-report_v3.pdf> [Accessed 6th November 2015].

Lewis, J.A (2014) Centre for Strategic & International Studies: **Underestimating Risk in the Surveillance Debate**. [Online] Available from:

<http://csis.org/files/publication/141209_Lewis_UnderestimatingRisk_Web.pdf> [Accessed 23rd November 2015].

Necessaryandproportionate (2014) **International Principles on the Application of Human Rights to Communications Surveillance**. [Online] Available from: <https://necessaryandproportionate.org/ > [Accessed 27th November 2015].

Petronio, S (2002) **Boundaries of Privacy: Dialects of Disclosure**. [Online] Available from: <https://books.google.co.uk/books?hl=en&lr=&id=8v89W_oJQ0wC&oi=fnd&pg=PR3&dq=boundaries+of+privacy+and+data+protection+will+be+redefined&ots=3Qh-k0mPxI&sig=dXHvJrJNF6Bq59d5VB-2zAukRjk#v=onepage&q&f=false> [Accessed 15th December 2015].

Polonetsky, J, Tene, O and Jerome, J. (2014) **Benefit-Risk Analysis for Big Data Projects**. [Online] Available from: <https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf> [Accessed 27th November 2015].

Preez, D.D (2015) **UK and US watchdogs warn of surveillance risks and the impact on society**. [Online] Available from: < http://diginomica.com/2015/01/07/uk-us-watchdogs-warn-surveillance-risks-impact-society/#.VlNecXbhCUl> [Accessed 23rd November 2015].

Privacy International (2015) **Two Years after Snowden: Protecting Human Rights in an Age of Mass Surveillance**. [Online] Available from: <https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN_0.pdf> [Accessed 27th November 2015].

Richards, N.M (2013) **The Dangers of Surveillance**. [Online] Available from: <http://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf> [Accessed 23rd November 2015].

Rudasill, L.M (2014) **The IFLA Trend Report and Library Horizons**. [Online] Available from: <http://eprints.rclis.org/25239/1/16-Reflexi%C3%B3n%2004.pdf > [Accessed 15th December 2015].

Sinclair, A and Annereau, S (2014) **Use of CCTV in the workplace in the UK: its roles and its risks**. [Online] Available from: <http://united-kingdom.taylorwessing.com/globaldatahub/article_cctv_roles_risks.html> [Accessed 27th November 2015].

Sottek, T.C and Kopstein, J (2013) **Everything you need to know about PRISM: A cheat sheet for the NSA s unprecedented surveillance programs**. [Online] Available from: <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> [Accessed 2nd November 2015].

Suski, E.F (2014) **Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority under Cyberbullying Laws**. [Online] Available from: < http://eds.a.ebscohost.com.ezproxy.leedsbeckett.ac.uk/eds/pdfviewer/pdfviewer?sid=4f1da458-bdc3-41e3-92f3-1244f93ca517%40sessionmgr4002&vid=1&hid=4102> [Accessed 27th November 2015].

Taylor, E (2011) **Awareness, understanding and experiences of CCTV amongst teachers and pupils in three UK schools**. [Online] Available from: <> [Accessed 27th November 2015].

Troy: Cyber Hijack, series 1 (2015) **Episode 1**. London: E4, 15 December, 21:00.

Wikipedia (2015) **Human Rights Act 1998**. [Online] Available from: <https://en.wikipedia.org/wiki/Human_Rights_Act_1998 > [Accessed 23rd November 2015].