

** INDIVIDUAL TASK COVER SHEET**

**ELPP Level 4**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Student, please sign, date and attach cover sheet to front of assessment task for all submissions* | | | | | | | | | |
| **SUBJECT CODE** | **LS0410/LS0411 – SP91 2019** | | | | | | | | |
| **STUDENT FAMILY NAME** | **STUDENT GIVEN NAME** | **JCU STUDENT NUMBER** | | | | | | | |
| **BERTOCCO** | THOMAS-KILLIAN | 1 | 3 | 7 | 5 | 8 | 3 | 2 | 2 |
| **ASSESSMENT TITLE** | **IN CLASS ESSAY 2 – Poster Essay** | | | | | | | | |
| **DUE DATE** | **12 April 2019** | | | | | | | | |
| **LECTURER NAME** | ***Thomas-Killian Bertocco*** | | | | | | | | |
| **TUTOR NAME** | n/a | | | | | | | | |
| **Student Declaration**   1. This assignment is my original work and no part has been copied/ reproduced from any other person’s work or from any other source, except where acknowledgement has been made (see *Learning, Teaching and Assessment Policy 5.1*). 2. This work has not been submitted for any other course/subject (see *Learning, Teaching and Assessment Policy 5.9*). 3. This assignment has not been written for me. 4. I hold a copy of this assignment and can produce a copy if requested. 5. This work may be used for the purposes of moderation and identifying plagiarism. 6. I give permission for a copy of this marked assignment to be retained by the College for benchmarking and course review and accreditation purposes.   [Learning, Teaching and Assessment Policy](http://www.jcu.edu.au/policy/allitoz/JCU_076643.html) 5.1. A student who submits work containing plagiarised material for assessment will be subject to the provisions of the [Student Academic Misconduct Requirements.](http://www.jcu.edu.au/policy/allitoz/JCUDEV_005375.html)  **Note definition of plagiarism and self plagiarism in Learning, Teaching and Assessment Policy:**  **Plagiarism:** reproduction without acknowledgement of another person’s words, work or expressed thoughts from any source. The definition of words, works and thoughts includes such representations as diagrams, drawings, sketches, pictures, objects, text, lecture hand-outs, artistic works and other such expressions of ideas, but hereafter the term ‘work’ is used to embrace all of these. Plagiarism comprises not only direct copying of aspects of another person’s work but also the reproduction, even if slightly rewritten or adapted, of someone else’s ideas. In both cases, someone else’s work is presented as the student’s own. Under the Australian *Copyright Act 1968* a copyright owner can take legal action in the courts against a party who has infringed their copyright.  **Self Plagiarism:** theuse of one’s own previously assessed material being resubmitted without acknowledgement or citing of the original.  **Student Signature**  **…………………………………………………… Submission date 12/04/2019** | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **INSTRUCTIONS TO STUDENTS:** |  |  |

|  |  |
| --- | --- |
| 1.  2.  3.  4.  5.  6. | Complete the Individual Task Cover Sheet.  Attach your prepared Essay Plan to the essay  You must write 800 words, +/- 10%.  Double-space your writing – write on every second line.  Submit the Essay Plan and completed Essay in Blackboard at Assessments. |

|  |
| --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **1st Marker** | | **2nd Marker** | |
| Organisational Structure | /30 | Organisational Structure | /30 |
| Range of Content | /30 | Range of Content | /30 |
| Vocabulary | /20 | Vocabulary | /20 |
| Grammar and Syntax | /20 | Grammar and Syntax | /20 |
| TOTAL | |  | |
| AGREED MARK | | | |
| Name | | Name | |
| Signature | | Signature | |



**ESSAY 2 – Poster Text**

**Bertocco Thomas-Killian / 13758322**

**ELPP 4**

**12/04/2019**

**Less privacy, more security.**

# Abstract

When the world population approaches the 8b of humans, and new type of threats appears, how can governments protect their countries against them. During our history, we always used spies to gather information about our enemies, prevent them to attack, or even control them.

Now that the number of religious, political, separatist groups increased drastically, it became impossible to assign an agent to all of them. An attack can come from a random citizen for a random reason, at a random place.

The 21 Century have been marked by the apparition of new technologies, and by the information revolution. Citizens from almost every country, even some of the poorest ones, use modern technologies to communicate. In addition, a lot of people share their personal information on different services (e-shop, social networks, games, …). The data became the opportunity to keep an eye one everyone. How can intelligence agencies gather and analyse it? Who are the targets? Which information do they take? More importantly, are they really using it to protect us?

Table of Contents

[Abstract 4](#_Toc6392091)

[Introduction 6](#_Toc6392092)

[I / How Governments gather private information? 7](#_Toc6392093)

[1 / The man in the middle 7](#_Toc6392094)

[2 / Hack data centers 8](#_Toc6392095)

[3 / Hack the target 8](#_Toc6392096)

[4 / Modify the law 9](#_Toc6392097)

[5 / The partnerships 9](#_Toc6392098)

[II / How do intelligence agencies analyse data? 10](#_Toc6392099)

[III / How does this mass surveillance threaten our privacy and freedoms? 11](#_Toc6392100)

[Conclusion 12](#_Toc6392101)

[References 13](#_Toc6392102)

[Essay Plan 14](#_Toc6392103)

# Introduction

Over the past decade, our methods of communication have evolved.

The Internet has become a mainstream tool of communication, used by more than 81% of people in developed countries.

New technologies have invaded our daily life: Sending a message to a friend, buying a book, moving around, etc. all our actions produce data that is then stored on private servers.

Also used by criminal groups/individuals, these networks have led to the multiplication of various threats. Sale of illegal products, dissemination of extremist ideas, harassment, incitement to hatred, child pornography, terrorism, the list is long.

In order to monitor these threats, some government agencies have developed very large-scale solutions for retrieving and analyzing data from the Internet.

Used by a democratic state, this information can be used to preserve the integrity of the territory and its citizens. However, this power can also be used for wrong purposes and become a dangerous weapon.

These highly controversial mass surveillance methods are entering our private lives to better protect us.

How and why governments collect and analyse your data?

# I / How Governments gather private information?

With the multiplication of websites and connected technologies, there are now many data sources available.

However, these sources remain inaccessible and belong to private companies.

There are therefore five ways to collect this information.

## 1 / The man in the middle

Two people communicate while a man listens to them, hiding behind a door.

The cables and antennas through which our information flows are easily accessible. It is therefore simple to install surveillance equipment to intercept data transiting your own territory.

The data flow collected by this method is considerable, however, this system has its limitations.

The recovered data is raw, which means that some data are understandable, some do not mean anything, and others are encrypted.

Most data are encrypted with complex algorithms, making it very difficult to decrypt and therefore unusable.

Secondly, it remains complicated to use this method outside its borders.

However, some countries do not hesitate to send agents to infiltrate foreign Internet providers, or even submarines, to intercept communications through submarine cables.

## 2 / Hack data centers

Accessing servers of multinational companies set up by teams of experienced engineers is not easy.

Difficult, certainly, but far from impossible, especially when you have a real army of experts in cybersecurity, artificial intelligence, and supercomputers.

The easiest way to access it is to use an undercover agent. However, most hacks are performed remotely, through the discovery of vulnerabilities and their exploitation.

It is interesting to note that most of the information will not be encrypted, as the companies that own it want to use it for marketing purposes.

## 3 / Hack the target

If the target is already identified, it is preferable and simpler to attack it's Android smartphone directly rather than penetrate google servers.

We all use widespread technologies such as Android, Windows, Ios, or Intel Cpu. Intelligence agencies have been collecting and using vulnerabilities related to these systems for many years to spy on people who are already defined as a potential threat.

## 

## 4 / Modify the law

Forcing companies to transmit their data is certainly the easiest method.

This solution is not recommended because it will cause protests, but also because it will encourage users to use encrypted communications solutions.

## 5 / The partnerships

Sometime when you need something, you just have to ask and give a lot of money.

So now is the time to talk about social networks.

Social networks are the main data sources for intelligence agencies in terms of the number of users but also the variety of information.

For these reasons, intelligence agencies and some specific websites have partnerships to access data in real time.

There may also be secret partnerships, for example Microsoft may voluntarily leave backdoors in its systems and share them with the CIA.

# II / How do intelligence agencies analyse data?

This large amount of data collected is also called Big Data.

Due to its huge size, it is impossible to analyse this information manually, so it is necessary to use artificial intelligence.

Machine learning is algorithms that parse data, learn from it, and then apply what they have learned make predictions or decisions.

By browsing the data tables, the AI will train and make statistics. The more information you have, the more accurate your AI will be.

To use this method, it is important that the information collected is relevant and related to the prediction.

For example, if I want to predict if someone is a terrorist, I need to know his salary, religion, last trips, number of children, nationality, etc.

This process is the most effective known to date, but many threats still fall through the cracks because of the excessive amount of data.

# III / How does this mass surveillance threaten our privacy and freedoms?

Intelligence agencies do not filter any data. Everyone is a potential threat, so everyone is being watched.

This constant surveillance forces us to self-censor. Sharing confidential documents, political opinions, religious affiliation, has become complicated in some countries for fear of reprisals from authoritarian governments. For example, 71% of internet users live in countries where ICT users were arrested or imprisoned for posting content on political, social, or religious issues (Freedom on the net 2018, 2018).

The most obvious example is China, which moderates and punishes many topics of discussion: criticism of the government, discussions on religious or ethnic minorities, pollical opposition, etc.

In addition, this data allows users to be classified into categories. It is therefore easy to target and persecute an ethnic, religious or political group. The effects of such a weapon in the hands of a fascist government could be devastating.

# 

# Conclusion

This mass surveillance has already proven on several occasions that it is effective and has made it possible to arrest many criminals. However, it is very often used to control and censor rather than protect. This system is not about to stop, and will even expand to new devices to collect even more information. Home automation, household appliances, connected cars, etc. all electrical appliances will become sources of information.

I think this technology is a huge threat to the net neutrality and our freedom of expression. In the current context, more and more countries are arming themselves and passing laws to increase the legality of monitoring telecommunications networks. De plus en plus de sujets sensibles / critiques deviennent interdits.

Unfortunately, there is no other way to monitor billions of people. It is also very complicated to target only suspicious individuals because the amount of data is too large. It is therefore difficult to judge whether to prohibit or encourage this type of monitoring.

# References

*Freedom on the net 2018.* (2018, october). Retrieved from freedomhouse.org: https://freedomhouse.org/sites/default/files/FOTN\_2018\_Final%20Booklet\_11\_1\_2018.pdf

Fry, J. D. (2015). Privacy, predictability and internet surveillancce in the U.S. and China: Better the devil you know ? *University of Pennsylvania Journal of In-ternational Law, 37*(2), 419-501.

Maras, M.-H. &. (2019). Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy, 1-18*. doi:10.1080/23738871.2019.1590437

Marthews, A. &. (2015). Government surveillance and Internet search behaviour. *Social Science Research Network*.

Verri, G. B. (2014). Government and corporative internet surveillance. *UFRGS Model United Nations*, 119-134. doi:2318-3195

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 37*(5), 618-627. doi:10.1016/j.clsr.2015.07z

# Essay Plan

NAME: Bertocco Thomas-Killian STUDENT #13758322 DATE 02/04/2019

TOPIC: Less privacy, more security

INTRODUCTION:Background / context: information revolution, crimes, wars, terrorism.  
Large territories, high population, protection  
Technology, surveillance

Thesis Statement: (reference to Body Topics)  
Governments + spy + analyze + security + privacy

BODY 1:  
Topic Sentence: Government + gather + informations.Methods  
.Which infomations  
. Protections  
. Examples

BODY 2:  
Topic Sentence: analyze + data + use.Big Data  
.Machine learning, AI  
.Possibilities  
.Examples

**BODY 3**:  
***Topic Sentence: menace + privacy + liberty***.Laws, ethics  
.Critics  
.Which impacts?  
.Examples

**CONCLUSION** (refer to Thesis Statement and Body discussion + Opinion):  
.Results  
.Personal opinion  
.Evolution