


Privacy awareness after the Snowden case

A case study conducted from a global perspective

Copenhagen Business School 2016



Student name	Martin Hechmann Thorsen
Student number	Math11ak / 85486
CPR	
Program	Cand.merc.(it.) IMBE
Signature	

The signature of the student testifies that all content is the student's own work and that all sources are referred to.

Type of paper or assignment	Master thesis
Title/subtitle	Privacy awareness after the Snowden case / A case study conducted from a global perspective
Due date for submission	2016-09-15
Name of supervisor	Robert D. Austin
Number of characters/pages	123.118 / 77 pages all incl.


Declaration of Authorship

(To be placed at page 2 in the assignment!)

Identification	
Title of assignment:	Privacy awareness after the Snowden case
Study programme:	Cand.merc(it) IMBE
Course:	Master thesis
Type of Exam (e.g. Home assignment or Bachelor Project):	
Master thesis	

Social Security No. or Student ID:	Name of author(s):	Group no. (if relevant)
	Martin HechmannThorsen	

Number of pages:
<p>According to the exam regulations for this particular exam, the assignment must be of a maximum of 80 pages (Insert max. number of pages) exclusive front page, bibliography and appendices. Appendices are not included in the assessment.</p> <p>Each individual page of the assignment may not comprise more than 2,275 characters (incl. spaces) on average. (E.g. similar to 35 lines of 65 characters). All pages must have a margin of min. 3 cm in top and bottom and min. 2 cm to each of the sides. The font must be of a minimum of 11 pitch. Tables, diagrams, illustrations etc. are not included in the number of characters, but will not justify exceeding the maximum number of pages.</p>

Code of conduct:	
<p>Undersigned author hereby declare:</p> <ul style="list-style-type: none"> - that I/we individually or together with the group members listed above have written and completed this assignment. - that I/we have indicated all quotes with quotation-marks and provided references to their sources. - that the assignment complies with all regulations stated above regarding size and form. 	
Date: 2016-09-14	Signature(s):
	

Abstract

Data from life on the internet is floating around and is used in many relations, whether for knowing something about others or paying for products and services. The leaks of Snowden back in 2013 caused attention to the aspect of mass surveillance against innocent people by governmental institutions such as NSA.

This thesis is based on a case study conducted over the Snowden case and based on this, determines whether any changes have been registered in the awareness of privacy concerns. This is seen from the paradigm of neo-positivism and in relation to surveillance, transparency and control with the last two expanded and modified in a new manner of looking at society. To clarify this, selective search terms are used with Google Trends and combined with number of uses of the privacy tools DuckDuckGo, Tor and Tails. Putting together these results with the chosen theory of Foucault and Panopticon, Maslow's Hierarchy of Needs, Gate Keeping Theory and Rational Choice Theory, this together aggregates a grounding for the analysis and discussion leading to the conclusion of the thesis. The findings suggest a short increase in the awareness of privacy concerns. Besides this, there is a picture of an increasing use of privacy tools from the Snowden case to today. Suggestions for further research are hereafter counted for.

Table of contents

Abstract.....	1
Introduction.....	6
Research question.....	6
Case description.....	7
Snowden case.....	7
Literature review	10
Privacy concerns.....	10
Social media vs. in-person communication	10
Data floating.....	12
Media and the role of being a gatekeeper.....	13
Political control	13
Social media	16
Delimitation.....	17
Clarification of concepts	19
Digital exhaust.....	19
Entity	19
Cross indexing	19
Transparency.....	20
Control.....	20
Introduction to new concepts.....	20
Super transparency.....	20
Extreme transparency.....	20

Super control	21
Extreme control	22
Theory	23
Foucault and Panopticon	23
Maslow's Hierarchy of Needs	24
Gatekeeping theory.....	25
Rational choice theory	27
Methodology	27
Literature research.....	27
Quality of the sources	28
Approach	28
Paradigm	28
Inductive reasoning.....	29
Research design	30
Case study	30
Data collection	31
Data collection tool.....	31
Uncertainties in search terms	32
Credibility	33
Validity	33
Reliability.....	35
Results.....	36
Google Trends	36
Privacy tools	47

DuckDuckGo.....	47
Tor.....	49
Tails.....	50
Analysis and discussion	51
Transparency.....	51
Something to hide?.....	52
Concerned about transparency?	52
Leaks = transparency?.....	52
Fear of missing out.....	53
Control.....	53
Control. Who benefits?	53
(Mass) surveillance?.....	55
Gatekeepers.....	59
Concerned about control?	59
Conclusion	63
Limitations of this research.....	64
Further research	65
Bibliography	67
Books.....	67
Articles.....	67
Webpages and online articles	68
Appendixes.....	I
Appendix 1 – Data never sleeps.....	I
Appendix 2 – Primitive privacy tools.....	II

Appendix 3 – Mobile penetration globally.....	III
Appendix 4 – Connected devices and future forecast	IV

Introduction

We are all being watched! This is a fear for many people in today's society and the big question is whether the Snowden case has changed people's awareness of privacy concerns.

There is no doubt about data being the new oil and data is floating. Businesses around the world earn huge amounts of money based on data. This data is collected because it gives value in several respects from different parties e.g. by having an assumption of personal information as an actual monetary value and for governmental use. This creates creative ways of getting access to people's data from several fronts of both businesses and government agencies. As a reaction to this, there are many privacy tools being developed but are they used at all?

From the literature explored, a gap is observed in the absence of studies combining people's interests according to Google searches and the use of privacy tools after a case of suspecting mass surveillance as seen in the Snowden leaks. This gap is filled by researching whether people are more aware of privacy concerns after the Snowden leaks and examined with a collection of data combined with a new perspective of a possible future scenario for society. This contributes to the understanding of people's acting and whether any changes can be noticed after the specific case.

New concepts are introduced with associated models for illustrating a new way of looking at society. These models consider and expand the existing understanding of "transparency" and "control" and put these upon the basic results from the data collected.

The thesis is conducted from a case study of the Snowden leaks with the purpose of examining any changes in awareness of privacy concerns. This is done using Google Trends and usage numbers for selected privacy tools DuckDuckGo, Tor and Tails and brings a profound analysis and discussion of the results combined. Further, relevant theories are used to contribute to the analysis and discussion of the results. In the approach of this research, the paradigm of neo-positivism is used as overall worldview and this is combined with an inductive reasoning.

The above creates the framework for the initial research question and this thesis' contribution to the knowledge base in this field. The final research question for this thesis sounds:

Research question

Examine whether the Snowden case has caused changes in the awareness of privacy concerns related to surveillance, transparency and control for users of the internet.

Case description

In the following section, the case used throughout the paper, is described. The case is of a recent date and it therefore reflects today's opinions and not least the issues we are facing today. The description below is exclusively reproduction of what has happened in the case and is included for giving a basic understanding of the main points of the case.

Snowden case

The Snowden case is a very well-known case of leaked documents from the US intelligence service National Security Agency (NSA). The case was first introduced to the public in the newspapers “The Guardian” and “Washington Post” on June 6, 2013. They reported that the NSA was monitoring millions of Verizon customers by collecting telephone records.¹ Other programs were also leaked which included NSA being able to extract audio, video, photos, e-mails, documents and much more from servers of big internet companies such as Microsoft, Google, Apple, Facebook, Yahoo and others with argues of “danger for terrorism”.¹⁵ Both “Washington Post” and “The Guardian” reported the program being far more invasive than anything seen previously. This program was called “PRISM” and would give direct access to a lot of people’s devices without warrants and thereby potential access to monitor the general public.²

A few days later, On June 9, 2013, “The Guardian” and “Washington Post” revealed that Edward Snowden was the leaker and that he was speaking from Hong Kong, explaining why he had done what he had done. At the same time, it was confirmed that Edward Snowden had been employed by the NSA for almost 3 months.¹

Snowden was fired for his actions and the reason given for this was “for violating ethics code”. This information was released on June 11, 2013. At the same date, the EU demands US assurances that the rights of people in Europe are not being infringed by this newly-revealed surveillance program.¹

In an interview in “The South China Morning Post”, published on June 12, 2013 Snowden further emphasized that U.S. intelligence agents have been hacking different networks all over the world for years.

The next day the FBI Deputy Director Sean Joyce alleges that one of the programs, called PRISM, has helped prevent a number of terrorist attacks as justification for monitoring people.¹

¹ https://www.whistleblower.org/snowden-timeline?gclid=Cj0KEQjwnv27BRCmuZqMg_Ddmt0BEiQAgeY1lxpkGQYwTF9sFwTUM-DqQDJbeeA_XNlpKtLXq-mDmvpcaAsYf8P8HAQ – 2016-07-08

² <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> - 2016-08-20

On June 14, 2013 a complaint containing a charge against Snowden for espionage and theft of government property.¹

By June 23, 2013 Russia was interfering in the situation when the Russian President Vladimir Putin verified that Snowden was in the transit area of Moscow's Sheremetyevo International Airport, causing the U.S government to revoke the passport of Snowden.¹

Days later by June 30, 2013 a German news magazine "Der Spiegel" reports that classified leaks by Snowden documents that NSA is monitoring European Union offices around the world, such as in Washington, New York and the EU building in Brussels.¹

July 1, 2013 Russia's official "RIA Novosti" news agency reports an asylum request from Snowden.¹

On August 1, 2013 the Russian lawyer "Anatoly Kucherena" now reports to "CNN" that Snowden has left the Moscow airport and that the application for political asylum for a year has been approved by Russia.¹

Months later, on November 3, 2013 a letter with the title "A Manifesto for the Truth" was published in the German magazine "Der Spiegel" purportedly written by Snowden. A major point of the letter was that "mass surveillance is a global problem and needs a global solution."¹

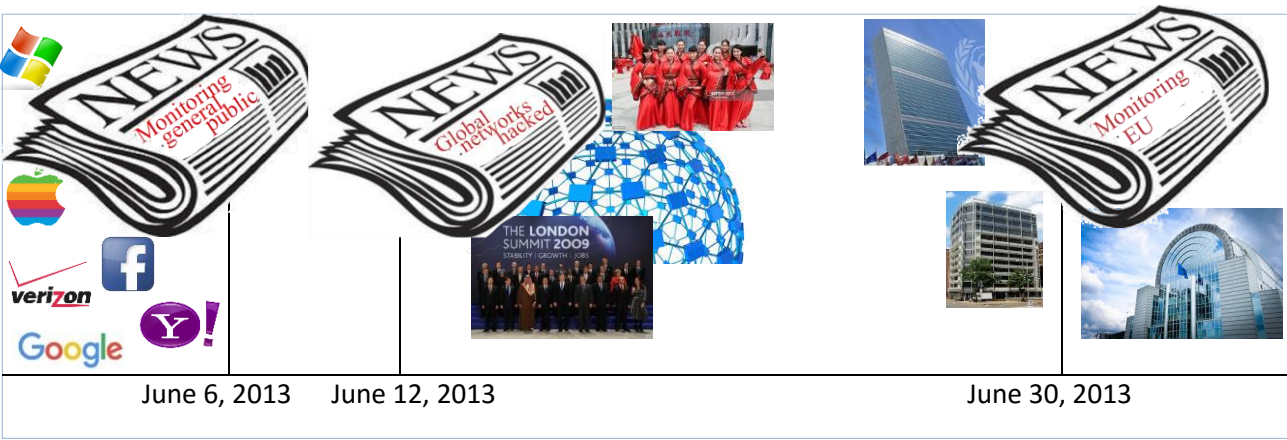
On January 23, 2014 Attorney General Eric Holder said: "If Mr. Snowden wanted to come back to the United States and enter a plea, we would engage with his lawyers." Snowden replied later that day, pointing out that returning to the U.S. is "unfortunately not possible in the face of current whistleblower protection laws".¹

On August 7, 2014 Snowden announced that he had been granted an extension to stay in Russia for three more years.

According to "CNN" claiming that Snowden wants to go back to the United States to serve his sentence for illegally leaking highly classified intelligence documents. His lawyers are ready for discussing a deal with the U.S government.³

³ <http://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/> - 2016-07-10

Illustration showing the Snowden case time span for three leaks important to this thesis:



Literature review

This section will provide an overview of existing literature on the subjects of this thesis followed by the delimitation.

This project was inspired by several readings related to the problem and some of them were chosen as the final inspiration sources.

Privacy concerns

One might expect that an exposé like the one of the Snowden leaks would, to some extent, increase the public's focus on privacy. This has, however, only been the case to a very limited degree. When compared to e.g. the reactions to news of a royal baby in the same period, the Snowden case only caused minor reactions, and only for a short while.

A cite from the study states:

*"My results challenge the assumption that Web users would start to care more about their privacy following a major privacy incident. The continued reporting on state surveillance by the media contrasts with the public's quickly faded interest."*⁴

Results show that visits to privacy related Wikipedia pages and privacy related webpages in general increased significantly but faded out after a short time. Tools for getting more privacy through anonymity like Tor, anonymoX, Private/Incognito settings in browsers and the search engine DuckDuckGo experienced a minor increase in use, as suggested by this quote:

*"Snowden's revelations brought few new users to privacy-enhancing technologies."*⁴

Of course the implicit problem of counting people using tools that help them be "invisible" or anonymous may affect these surveys.⁴

Social media vs. in-person communication

Studies show a significant difference in the communication of face-to-face and on social media when looking at surveillance and the Snowden case. This has to do with the fear of disagreeing with the recipients of the opinions shared and hence fear of standing out. The same opinion about the Snowden case

⁴ Preibusch, Sören. (2015) *Privacy Behaviors After Snowden*. Communications of the ACM

would gladly be expressed by 86% in a study conducted by Pew research in 2014, in an offline forum such as at a family dinner, restaurant with friends etc. Less than half of these people would share the same opinion about the Snowden case online because of the fear of disagreement with the receivers.⁵

Another famous study which confirms the fear of standing out, was performed by psychologist and professor Solomon Asch and is described in the following:

*"In the Laboratory of Social Relations at Harvard University. Seven student subjects are asked by the experimenter to compare the length of lines. Six of the subjects have been coached beforehand to give unanimously wrong answers. The seventh has merely been told that it is an experiment in perception"*⁶

The result is surprising:

*"Under ordinary circumstances individuals made mistakes less than 1 per cent of the time, but under group pressure the subjects accepted the wrong judgments in 36.8 per cent of the cases."*⁶

Besides this, the spreading of information through the media can result in an overestimated view of an opinion which can support a minority view. This is called "Spiral of Silence" and creates a condition of pluralistic ignorance from a story, too narrowly covered by the media.⁵

Much doubt lies in the speculation about whether the monitoring is performed and thereby whether the individual person is being watched by someone. This further emphasizes the idea that people are less talkative when monitored as suggested in this cite:

*"...when individuals think they are being monitored and disapprove of such surveillance practices, they are equally as unlikely to voice opinions in friendly opinion climates as they are in hostile ones."*⁷

The above idea, though, is not in line with other studies conducted before the Snowden case occurred. One study had results based on cross sectional survey data which can only provide correlational, not causal, evidence. The idea is based on the fact that people who were monitored by the government (52% in 2003), with possessed minority opinions, would also be the ones to share their opinions on social media platforms.⁷

⁵ Hampton, K.N., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social Media and the 'Spiral of Silence*. Pew Research Center.

⁶ Asch, E., Solomon (1955). *Opinions and Social Pressure*. Scientific American

⁷ Stoycheff, Elizabeth (2016). *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*. Journalism & Mass Communication Quarterly.

Low self-esteem also has an effect on people's likeliness of sharing things. This is seen in a study by Noelle-Neumann:

*"Low self-esteem will cause a person to remain mute. Noelle-Neumann's research team identifies these individuals by their agreement with a survey statement about relationships: I know very few people."*⁸

Data floating

One of the core parts of the overall idea of this paper, is concerning data and information flows. Data has been called "the new oil" with big rewards for the ones who see the opportunities in extracting a meaningful output. From this idea, we have the "good data beats opinion"-philosophy arguing that the right way to operate goes through truly understanding data as a base for facts rather than going with "gut feelings".⁹

The value in data today lies in the micro data and not macro data and this is why much data is collected about every individual.¹⁰ This is seen in the permissions to approve when downloading apps on smartphones, such as tracking of location, use of cookies on the web, asking people for their opinions and much more. An important question intrudes: Who knows what about me and do they know more than I have informed?

Our everyday lives become increasingly more digital. Transactions, messages, activities etc. not only generate data, but the amounts and details of this data is also increasing. These so called "digital footprints", can link a person's doings years back and follows the idea of "the internet never forgets"¹¹.

All these data have become one (or several) big pool(s) of floating data spreading between persons, service providers, governments and other entities, and no one knows who has which data and even more data can be generated from derivation of data. This spreading is much in line with the media as seen below.

⁸ Noelle-Neumann, Elisabeth (1993). *Spiral of silence*. McGraw-Hill.

⁹ <http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> - 2016-07-17

¹⁰ http://data.library.ubc.ca/guide/whats_difference.html - 2016-07-17

¹¹ https://www.ics.uci.edu/community/news/articles/view_article?id=217 - 2016-08-20

Media and the role of being a gatekeeper

The term “media”, in this context, includes both the traditional press and the social media. The press is a big player in spreading the word and is in many ways defined as a gatekeeper (see section “Gatekeeping theory”) of stories because the newspapers, television stations etc. decide what stories to run with. The fact that one entity has the power to decide what should be spread, can be dangerous because a tempting lure of misuse this control is present.¹²

Stories about privacy concerns covered by printed media tend to be negatively biased, as documented by an analysis of the coverage of concerns over consumer privacy in printed media during the period 1990 – 2011. In the traditional media, negatively loaded stories outweighed positive or neutral stories by 3:1. According to this, people see print media as more reliable than broadcast media.¹³

In some situations, a social media platform itself is the distributor of a story and this would make the platform the gatekeeper.

When news is shared on social media platforms by individuals, some would argue that the gatekeepers are too influential in deciding what should be spread.

In many countries like North Korea, Burma, Turkmenistan, Equatorial Guinea, and Libya, the media are censored and controlled. These are all on the list of the 10 most censored countries in the world, with North Korea topping the list.¹⁴

Political control

Through censorship and general control over media, governments in less democratic countries holds a lot of influence over what is published and hence over what information the public has access to.

In democracies, freedom of speech and specifically having a free press is considered a fundamental truism. Though freedom of speech is essential to democracy, does it also guarantee transparency, e.g. of political decisions and their backgrounds?

Also, in what ways do politicians in democracies attempt to control what is publicized and to what degree does this control limit the experienced transparency? What kinds of restrictions to transparency are ac-

¹² <https://www.utwente.nl/cw/theorieenoverzicht/Theory%20Clusters/Media,%20Culture%20and%20Society/gatekeeping/> - 2016-08-25

¹³ Roznowski, L. Jo Ann. (2003) *A CONTENT ANALYSIS OF MASS MEDIA STORIES SURROUNDING THE CONSUMER PRIVACY ISSUE 1990-2001*. Wiley InterScience.

¹⁴ <https://cpj.org/reports/2006/05/10-most-censored-countries.php> - 2016-07-20

ceptable for instance in the interest of successful trade negotiations? For instance, transparency will naturally be limited, when it comes to e.g. a government's anti-terrorism monitoring of its own citizens and of other countries.

This monitoring of the public is in itself an example of political control practiced more and more by governments even in democracies, and one that is often the source of bitter arguments.

"Some 57% say it is unacceptable for the government to monitor their communications"¹⁵

As a picture of the ambivalence of people's views on this topic, the study also concludes that 82% of the citizens of the United States believe that surveillance of people suspected of having a relation to terrorism is necessary in the current security situation. 40% of the population in the United States find it justifiable to surveil ordinary U.S. citizens. Furthermore 60% of U.S. citizens think the communication of American leaders is acceptable to monitor.¹⁵

The Snowden leaks, revealing a degree of control by NSA, not realized by the public, has functioned as a catalyst for a discussion of the problem with the lack of transparency in this area.

Pro-surveillance advocates have several arguments supporting their stance. One argument often encountered is the "nothing to hide" argument:

"These findings exemplify a behavioral manifestation of the "nothing to hide" argument often advanced by proponents of Internet surveillance. Those who feel the government is justified in surveillance activities argue their behaviors may be monitored because they are not trying to hide any wrongdoing..."⁷

This argument is typically countered, as in this continuation in the same source:

"...Contends that individuals' fundamental need for privacy is not necessarily grounded in concealing wrongdoing, but rather in "concealing information about themselves that others might use to their disadvantage." Understood this way, nearly everyone has something to hide."⁷

Similar to the Snowden case, the decision of having session logging in Denmark, which politicians currently consider reintroducing¹⁶ is also an example of control in the form of mass surveillance.

¹⁵ Rainie, Lee & Madden, Mary. (2015) *Americans' Privacy Strategies Post-Snowden*. Pew Research Center

¹⁶ <https://edri.org/danish-government-plans-to-re-introduce-session-logging/> - 2016-07-20

The distinction between surveillance and mass surveillance lies in whether the persons being surveilled are selected through some criteria directly relevant to a threat or whole populations or groups of populations surveilled without specific suspicions.¹⁷

When naming his famous book “No place to hide” Glenn Greenwald was inspired by the suggestive quote from Senator Frank Church:

“The United States government has perfected a technological capability that enables us to monitor the messages that go through the air.... That capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn’t matter. There would be no place to hide.”¹⁸

Controlling people through surveillance has to do with knowing as much as possible about their doings and is often introduced with reference to a threat of terrorism.¹⁵ This modus operandi gained momentum after the terrorist attack on September 11, 2001 and has been steadily fortified since.¹⁸ This extended use of surveillance has been confirmed by the Snowden leaks¹, though president Obama, when asked about NSA in the “Tonight Show” in 2013, denied it:

“We don’t have a domestic spying program. What we do have is some mechanisms that can track a phone number or an email address that is connected to a terrorist attack.”¹⁸

An article in New York Magazine reveals that, while terrorism is often used a chief argument for escalating surveillance, in reality, the surveillance is primarily used for solving ordinary crimes:

“New York magazine revealed that from 2006 to 2009, the “sneak and peek” provision of the act (license to execute a search warrant without immediately informing the target) was used in 1,618 drug-related cases, 122 cases connected with fraud, and just 15 that involved terrorism.”¹⁸

Terrorism has become a topic of interest to many, despite the fact that the number of people killed by “Muslim-type terrorists” outside warzones basically is the same as the number of people drowning in their bathtubs each year. This comparison may provide a little perspective on this hyped topic, often used by governments as argumentation for surveillance.¹⁸

The view on being surveilled by the government varies, and some feel that “my life is too boring to follow” or “I really doubt that the NSA is interested in me”. People who share this view either deny that the

¹⁷ <https://www.privacyinternational.org/node/52> - 2016-09-10

¹⁸ Greenwald, Glenn. (2014) *No place to hide – Edward Snowden, the NSA and Surveillance State*.

surveillance is happening, do not care about the surveillance, or are simply willing to accept it. A quote from MSNBC from Lawrence O'Donnell further elaborates this idea:

*"My feeling so far is ... I'm not scared ... the fact that the government is collecting [data] at such a gigantic, massive level means that it's even harder for the government to find me ... and they have absolutely no incentive to find me. And so I, at this stage, feel completely unthreatened by this."*¹⁸

Other than the sheer amount of data collected about people by intelligence agencies, the types of data is at least equally interesting. NSA, for example, collects a wide range of information about the people they survey, including political views, medical history, intimate relationships and online activity. This information is claimed to be kept safe and the agency also claims that they are not abusing this information. ACLU's deputy legal director, Jameel Jaffer believes that this power potentially could be misused.¹⁸

The collection of our digital footprints, as performed by many private companies, can also be viewed by as a kind of mass surveillance. This is elaborated on in the next section.

Social media

Almost everything done on the web is logged and stored for every person. People use social media platforms as never before and generate data almost wherever they are with pictures, messages, status updates, locations and much more.

The amount of data generated in social media is growing by incomprehensible amounts each minute.¹⁹ (See Appendix 1 – Data never sleeps). Much of this data is defined as "open data" and is therefore accessible to everyone (or at least to everyone, capable of finding and making sense of this data) effectively contributing to the overall transparency of society.

The attention given to the fact that information about oneself is the real price paid, when signing up for a "free" service, is almost non-existent. Indeed, it is often overshadowed by the prospect of having access to a service such as being able to search for information on the web, having an email service, getting help to navigate etc. The point to notice is that nothing is for free as expressed by economist and Nobel Prize winner, Milton Friedman:

*"There ain't no such thing as a free lunch".*²⁰

¹⁹ <https://www.domo.com/blog/2015/08/data-never-sleeps-3-0/> - 2016-07-20

²⁰ The Oxford Dictionary of American Quotations. Hugh Rawson, Margaret Miner. 2006. P. 208

It will be interesting to see, one day, what potential the use of these data will demonstrate. Maybe we have only seen the tip of the iceberg when it comes to what all this data can be used for? A small hint at the possibilities of this kind of data analysis (data mining) can be found in the story of a father who discovered that his daughter was pregnant after he wondered about the targeted advertising she received.²¹

The right to have digital privacy is no longer a social norm because data is worth money and thereby used as means of payment for services. Big firms such as Google, Facebook, Apple etc. earns a lot of money of these data and a very typical answer of being against surveillance is the “nothing to hide” statement.¹⁵ This is also supported by the Googles CEO Eric Schmidt in 2009 to CNBC with the following quotation:

“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”¹⁸

Delimitation

Based on the above issues, is seen interesting trends and especially highlights tend to stir up in problem areas. This can be narrowed down to a clear delimitation of the problem, which leads to the final research question of this paper.

The first clear delimitation is based on the geographical aspect. In this paper, the focus will be based on almost the whole world, primarily the United States. Even though the data are global, using Snowden as case, naturally focuses on an American or western perspective.

Another thing which is delimit from, is related to the basis of the research which is based on a case study. The delimitation lies in the choice of only one case chosen. This case is the Snowden leak which is a great example of a past history event with good relations to governmental control and thereby with a political aspect included. The really interesting thing in this case, is the entire research of finding out whether this event has had any effect on the fair image of reality in the western world today.

A third delimitation is seen in the collected data. This paper does only takes existing data into account. By this means searches on the web. As search engine, Google is chosen because Google is definitely the most used search engine which stands for 64% of all searches in the US seen in one of the latest com-Scores.²² Specifically, Google Trends has been used for collection of data on search activity.

²¹ <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#175b9ed334c6> – 2016-09-10

²² <https://www.comscore.com/Insights/Rankings/comScore-Releases-February-2016-US-Desktop-Search-Engine-Rankings> - 2016-07-21

When only concrete searches on Google and numbers of searches on DuckDuckGo are used in this study, naturally people who do not use these services are not included.

Tor and Tails have been selected as representatives for a secure communication media and a secure operating system.

Clarification of concepts

In this chapter, the concepts used throughout the thesis, will be defined and clarified for creating a better understanding to build upon, later in the thesis. The following sections will be supplemented with illustrations modelling the important points. The focus of these definitions and illustrations is to clarify their meaning specifically in relation to the thesis, or if they differ from meanings used elsewhere.

Digital exhaust

Digital exhaust and digital footprints are used interchangeably throughout this thesis. They represent the data traces or “evidence” which can be linked to an individual or online presence as:

“Digital footprints of every actions performed on the web. The footprints can either come from the user taking an active part in the process, because of services picking up data about the user or third parties contributing with data about the user.”²³

When digital exhaust is crossed between different “entities”, we find the concept of “cross indexing” which are both described below.

Entity

The term “entity” covers the following in this paper: An organization or individual with authority or right to collecting and/or storing information about one or more persons. Examples of entities are companies like Google and Facebook, governments and individuals.

Cross indexing

Cross indexing is the act of combining the digital exhaust from several sources, and thus gaining knowledge beyond the sum of the sources.

If for instance a search on Google for “BMI” was performed by the same person buying a pair of running shoes on Amazon, this might imply that the person would be interested in starting a subscription to Sports Illustrated.

²³ A definition made of inspiration from: <http://www.internetsociety.org/your-digital-footprint-matters> - 2016-07-16

Transparency

A ground idea in this thesis is the definition of transparency. Transparency is defined: Transparency is making sure anybody can find and understand all data and reasoning behind decisions and actions as well as all data necessary to get a full picture.

Control

Control, as defined in this thesis, is the potential power over other people, gained through the possession of knowledge about these people. It is related to transparency in their common basis in information, but where transparency is about information available to everybody, control may be based on information, not shared with others.

Introduction to new concepts

For the purpose of this thesis, two new variations over each of the concepts Transparency and Control is introduced, to be discussed in the analysis and discussion.

Super transparency





Transparency brought to the next level. Here the stakeholder finds transparency in every aspect of his or her life.

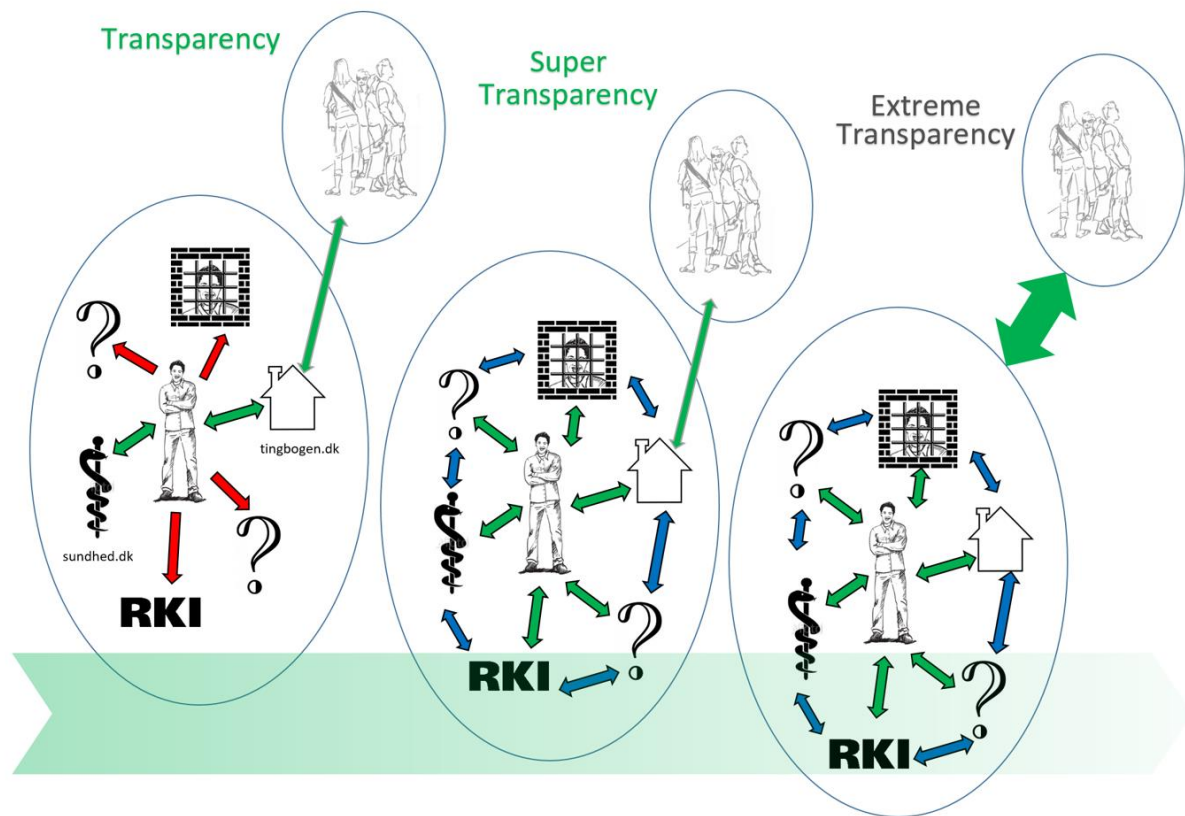
This is the theoretical situation where a person experiences complete transparency in every aspect of their life, i.e. has access to any information relevant to themselves, or specific defined: All information relevant to a person, can be found by this person.

Super transparency could provide answers to questions like: “Why are the politicians making their decisions and why are the laws as they are?” and “why are these commercials being shown in my browser?”

Extreme transparency

The even more theoretical situation where anyone can find any information about anyone. This is concrete outlined: “All information relevant to anyone, can be found by any person.”

Symbols	Description
	One-way information flow
	Two-way information flow
	Cross indexing
	Pointing towards more transparency as the color gets more transparent
Pictograms	Entities which are both private and national owned
Smaller sized circle with several persons	Everybody else in the society besides the person himself/herself



The Transparency circle on the left symbolizes the current situation, where a person has partial insight into his own domain.

In the Super Transparency circle a person has complete insight into his own domain.


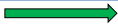


Finally, in the Extreme Transparency circle, everybody has unlimited insight into everybody's domains.

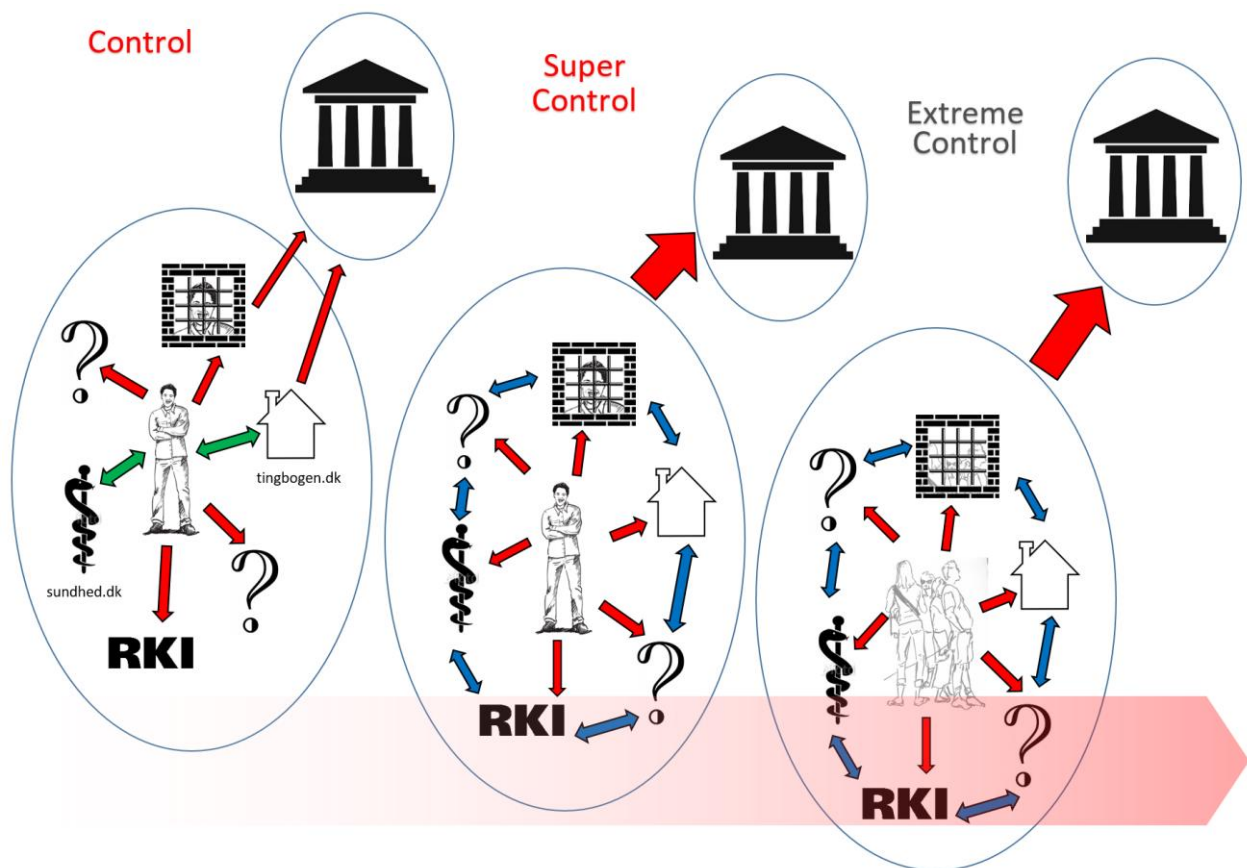
Super control

The theoretical situation, where an entity has all information about a person which is outlined: All information about one person is held by an entity.

Extreme control

The very theoretical situation, where an entity has all information about all people. Shortly defined: All information about everyone is held by one entity/person.

Symbols	Description
	One-way information flow
	Two-way information flow
	Cross indexing
	Pointing towards more control as the color gets more painted
Pictograms	Entities which are both private and national owned
Smaller sized circle with building	One entity or person



The Control circle on the left symbolizes the current situation, where information about a person is held by an entity which shares nothing.

In the Super Control circle, all information about a person is held by an entity which still shares nothing.

In the Extreme Control circle, all information about all people are held by one entity knowing everything about everybody while sharing nothing.

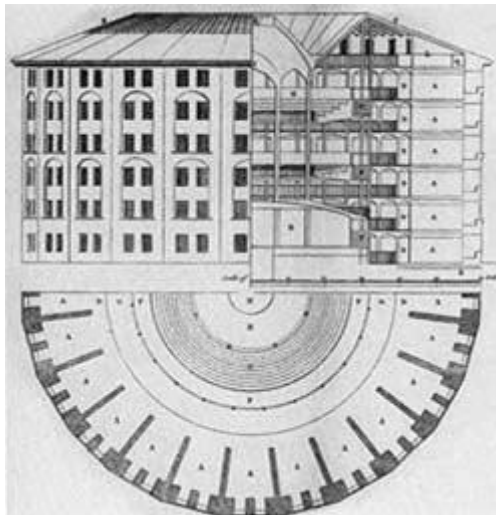
Theory

In this chapter the chosen theories are presented. The theories are placed in a separate chapter, and not as part of the literature review, to give a clear separation of the theories from the research literature.

Foucault and Panopticon

The French philosopher Michel Foucault (1926-1984) talks in his work “discipline and punish” about power in modern society and he believes that the idea of Panopticon is the ideal form of modern power.²⁴

Panopticon is a prison model created by the English philosopher Jeremy Bentham (1748-1832). The idea behind Panopticon is having a high degree of control over the prisoners with a minimum of staff. The prison is built, so that the prisoners are in separate cells with no view to each other's cells. The cells are placed in a circle around a tower which is placed in the middle. From the tower there is a monitor which is able to look into any cell at any time.²⁴ Panopticon is illustrated in the picture below.



25

The principle is that the prisoners do not know when they are being watched by the monitor. Foucault states that this situation with the permanent visibility of the prisoners gives power to the observer. His

²⁴ Gutting, Gary (2005). *Foucault: A very short introduction*. Chapter 8: Crime and punishment. Oxford University Press.

²⁵ <http://www.csub.edu/~sledford/> (08-09-2016).

theory is that the Panopticon prison model has spread to the modern society, in that the modern society now consists of many power relations like Panopticon.²⁴

Foucault further explains about how power systems get information from people (like in an examination or at a hospital where data is gathered and documented) and can control and use the information to formulate categories etc. getting new knowledge about people. This knowledge gives the power system a power and control over the people, which is basically the same principle as with Panopticon.²⁴

A major point of the original theory is the improved behavior of the convicts as a result of their knowing that they are being monitored. Since people do not have the same concrete sense of being monitored on the internet, the effect must be expected to be lower.

The theory can be used to analyze and discuss especially the transparency and control part of the research question since NSA has been gathering data about people through surveillance without their knowledge and people are leaving a lot of data behind due to the increasing use of the internet (see “data floating” section in literature review).

Maslow's Hierarchy of Needs

Maslow's hierarchy of needs is a very broadly known theory about the dependency between different levels of needs. The theory was founded in 1943 by Abraham Maslow and is a motivational theory.²⁶ Maslow believed that there are five basic needs: Physiological need, safety need, social need, esteem need and the last one is the need of self-actualization.²⁷ The needs are explained shortly in the following:

The physiological need covers the most basic needs as thirst, sleep, food etc. According to the theory, this need must be fulfilled to a high degree, before having the need on the next level.

The safety need is the second level and is about people having to feel secure both on a physiological and emotional level.

The social need arises when the safety need is reasonably fulfilled and is about people having to have some sort of connection and emotional bond to other people.

The esteem need is about people wanting to feel some kind of prestige, and it presents itself, once the social need is reasonably satisfied.

²⁶ <http://www.simplypsychology.org/maslow.html> - 2016-08-09

²⁷ Jacobsen, Dag Ingvar Jacobsen & Thorsvik, Jan (2008). *Hvordan organisasjoner fungerer*. Hans Reitzels Forlag. P. 213-214.

Finally, **the self-actualization need** has to do with reaching and using one's potential.²⁷



Though the theory is an acknowledged theory it is also an old theory and it has received critique on several points:

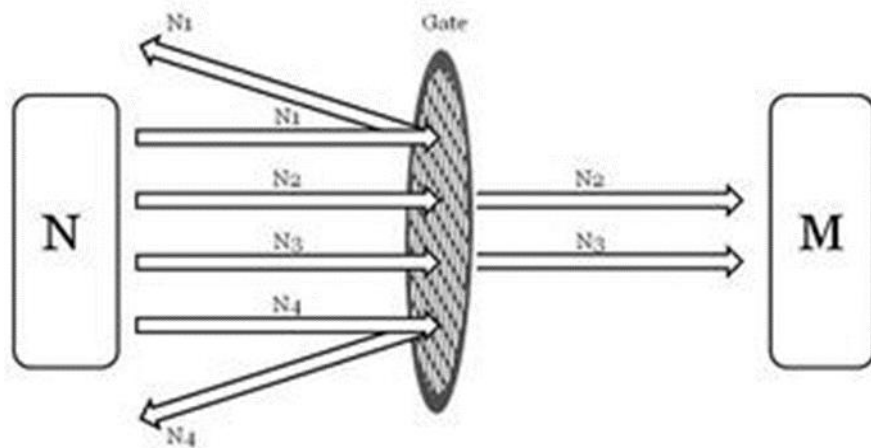
1. Being based on a method which is too subjective, the theory cannot be defined as a scientific fact.
2. Different cultures are not taken into account.
3. The criteria for reaching a higher level in the hierarchy is too rigid. For example, it has been argued that people who live in poverty and may starve, still can feel the need for love and having social relationships. According to Maslow this cannot happen.²⁶

The reason why Maslow's Hierarchy of Needs is relevant to this thesis, is that it explains people's needs for being social and belong to a group. It can be used to discuss why people may react the way they do based on the hierarchy of needs. The social need is what is relevant to discuss.

Gatekeeping theory

Originally the theory of "gatekeeping" was defined by a German psychologist, Kurt Levin, and the associated model is shown below:

²⁸ <http://www.bbc.com/news/magazine-23902918> - 2016-08-09



29

N = source of news item

N_{1,2,3,4} = News items

N_{2,3} = Selected item

M = Audience

N_{1,4} = Discard item

The model is simple in its core form and the idea comes from Levin's description of a mother which decides what food should end up being served on the family table.

In relation to the topic of this thesis, a gatekeeper is an entity or system, formally or informally trusted with the authority to function as a filter in the flow of information.³⁰ Examples of gatekeepers include editors in news media, bloggers writing about a specific topic and an automated system filtering stories on a social media platform.

The theory of gate keeping has been criticized for: The source being evaluated by a gatekeeper depends on the gatekeeper's subject area and can be all kinds of information.

Due to the generic nature of the gatekeeping process, the unlimited number of sources and the diverse types of gatekeepers, it is not possible to provide a description of how the filtering is performed.³⁰

In this thesis, the theory is relevant in relation to the media as gatekeepers in the case study. Since the emergence of social media, the role of gatekeeper has been expanded to include e.g. bloggers, celebrities and other non-professionals.

²⁹ <http://gatekeepingtheory.weebly.com/> - 2016-08-25

³⁰ Nahon, Karine. (2009). *Gatekeeping: A critical review*. Annual Review of Information Science and Technology. P. 27-28

Rational choice theory

The theory of rational choice is about personal profit maximization and is also called by other names, depending on the situation it is used in. It is a basic economic theory, derived from the idea that people are driven by an urge for personal gain and that they will aim for maximizing their own utility (personal satisfaction) as the fundamental basis of every action and decision made.³¹

The theory is criticized for being too universal as an explanation to fit any set of events independent of the situation. The problem lies in using “utility” as the driver, since this cannot be observed and hence, can explain any action and so adds no value to explaining why a person will do something.³²

In spite of the criticism, the theory is useful in analyzing and discussing what motivates people.

Methodology

The following chapter will describe the considerations about the methodology of this thesis. First comes a description of the literature research followed by a description of the approach including the choice of paradigm and research design. Next the data collection and processing will be described, and in the last part of the methodology section the validity and reliability of this thesis will be outlined.

Literature research

During the literature research both systematic research and chain research has been used. The chain research has itself been based on systematic research using references found in one piece of literature pointing to other pieces where new literature has been found by using the references from other literature.³³

The systematic research has been done by combining different keywords in different search databases. The chosen keywords are “Snowden”, “NSA”, “leak”, “privacy”, “awareness” and “security”. The keywords have been used separately and in different various combinations. They have been used in search databases such as EBSCOhost (Business Source Complete) and Cambridge Journals Online.

Only articles published in English have been included and thus only the English versions of the above keywords have been used in searches.

³¹ Brickley A., James, Smith W. Clifford & Zimmerman L. Jerold. (2009 fifth edition) *Managerial Economics and Organizational Architecture*. McGraw-Hill Irwin P. 22-23

³² Hodgson, M. Geoffrey. (2012) *On the Limits of Rational Choice Theory*. University of Hertfordshire Business School, UK

³³ Rienecker, Lotte and Jørgensen, Peter Stray (2011). *Den gode opgave*. Samfundslitteratur. P. 208-211.

It has set as criteria that the articles had to be in English, therefore the keywords are also only entered in English.

The articles have then been selected from their relevance to answer the research question.

Quality of the sources

This thesis uses literature from both primary and secondary sources. The secondary sources of this thesis are primarily books providing an overview of a given theory, and articles being used to describe the case.

Focus has been on using primary sources as much as possible throughout the thesis to ensure a higher validity.

When choosing literature, the author of the source and how well substantiated the article or book was, has been scrutinized to ensure a higher level of validity.

Approach

This thesis tries to examine whether awareness regarding privacy concerns has changed since the Snowden case. It aims to investigate and discuss the awareness in relation to surveillance, transparency and control with the Snowden case as the focal point.

To investigate this, the thesis has been structured in the following way: First a literature research chapter looks at existing literature on the subject and examines which areas of the subject have not been investigated.

Next a data collection, with the Snowden case as focal point, has been made and findings was analyzed and discussed with references to relevant theories on the subject.

In the following section, the approach, used for processing and analyzing the data is explained. Its effect on the analysis and the results is also elaborated on.

Paradigm

A paradigm is a worldview used as a perspective of the research. Of the four paradigms; positivism, pragmatism, critical and interpretive paradigm, the positivistic paradigm seems to have the best fit for this thesis' research. Arguments for and consequences of the choice of paradigm is explained below, along with a description of the positivistic paradigm.

Positivist or neo-positivist paradigm

The positivist paradigm relates to what can be observed and measured, and is used to find patterns and to make generalizations. It is based on logic and is often used in math-based professions. The positivist paradigm requires that the theoretical statement can be verified through experience (empiricism).³⁴

Positivism tries to find the exact truth and be fully objective, which it has been criticized for. Other paradigms believe this cannot be done. An extension of positivism is neo-positivism, which is in line with other paradigms on the idea that human values and emotions have to be taken into consideration, prohibiting the researcher from being completely objective.³⁵

The search terms chosen for collecting data for this research, will always contain some subjectivity from the researcher's side; when integrating the theories to the analysis and discussion, the human values and emotions will be a part of it. Therefore, this thesis ends up using a neo-positivist paradigm.

When choosing a paradigm, it has three different consequences for the science of the research. It has an ontological consequence, which has to do with the perception of reality, leading to a consequence for the epistemology, having to do with how you reach knowledge. Finally, this has consequences for the methodology, i.e. the method used to answer the research question.

Selecting the neo-positivist paradigm for this thesis, makes the epistemology modified objective and the method modified experimental/manipulative.³⁶

Inductive reasoning

When discussing the approach, it is to be defined whether an inductive or deductive reasoning is used.

Deductive reasoning is defined as:

"Deductive reasoning, or deduction, starts out with a general statement, or hypothesis, and examines the possibilities to reach a specific, logical conclusion".

And inductive reasoning is defined as:

³⁴ Birkler, Jacob (2005). *Videnskabsteori – en grundbog*. Gyldendals bogklubber. P. 52-57.

³⁵ Vøgted, S. (2006). *Valg der skaber viden – om samfundsvidenskabelige metoder*. P. 56-57.

³⁶ Vøgted, S. (2006). *Valg der skaber viden – om samfundsvidenskabelige metoder*. P. 53-55.

“Inductive reasoning makes broad generalizations from specific observations. ‘In inductive inference, we go from the specific to the general. We make many observations, discern a pattern, make a generalization, and infer an explanation or a theory.’”³⁷

This thesis is based on an inductive reasoning because the task of finding patterns and making generalizations is used in the research. Working inductively, correlates with the paradigm of neo-positivism.

Research design

The design of this research is built on a quantitative method, based on data related to the Snowden case and collected from Google Trends. The data collection will be described in the section “Data collection”. Next follows an elaboration on the case study and the reasoning for choosing a case study will be deepened.

Case study

First, a case study will be defined. According to Robert K. Yin a case study is defined as follows:

“A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.”³⁸

In this thesis, it is the effect (if any) that this case has had on people, more than it is the case itself, which is being investigated. The case has an essential role in the research, making the thesis a case based research.

Robert. K. Yin continues the definition with:

“The case study inquiry copes with the technically distinctive situation in which there will be many more variables of interest than data points, and so one result relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result benefits from the prior development of theoretical propositions to guide data collection and analysis”.³⁸

This thesis wants to research whether people have become more aware of privacy concerns, and to do this, it uses the Snowden case measuring if people’s attention were brought on to surveillance.

³⁷ <http://www.livescience.com/21569-deduction-vs-induction.html> - 2016-09-10

³⁸ Yin, Robert K (2009). *Case Study Research – Design and Methods*. SAGE Publications Inc. P. 18.

The Snowden case was very extensive and is therefore a good focal point when collecting data, to see if any difference in people's actions according their privacy can be seen. Data from the case is used in combination with data from the literature review and the collected data, thus there are multiple sources to analyze and discuss from.

Data collection

In this section an explanation of the data collection is given, along with which tools have been used and which search terms were chosen and why.

DuckDuckGo is an anonymous search engine and from this site, data about their traffic has been collected, to see whether there has been an increase, decrease or stagnation in number of searches. The same goes for Tor (a browser helping with keeping the user anonymous), but with the data from Tails (an operating system helping with keeping the user anonymous) the information is gathered through other literature. These tools have been chosen to include in the study, the kind of people, who has a better understanding of the issues related to the Snowden case as opposed to people using "normal" search engines etc.

There has been one collection tool to retrieve data about people's internet browser searches. This will be discussed in the next section.

Data collection tool

To collect data Google Trends has been used to see if there has been a change in searches about relevant topics after the Snowden case. The reason for using Google is that it is one of the world's biggest search engines and therefore can give a more generalized picture than some of the smaller search engines.

In Google Trends there can be inserted a keyword and typed a date range, and then it gives a graph over the searches of the given keyword. The graph takes point in the highest search number and shows the graph in percentage from this. Unfortunately, Google Trends does not give the exact number of searches, so there has been chosen a word where there is an approximately number to compare the result from the keywords with. The graph then scales according to this point.

The keywords and the selection of these are explained in the following.

Search terms

Through a massive readings of literature on related topics the search has been deduced.

Different search terms have been typed into Google's search engine to see if the results fit for what it is expected people would be searching for according to gardening their privacy on the internet. Then the key words have been chosen out from this. There has also been chosen search words about the Snowden case itself to see if people have had interest for the case, this to compare with the other results.

In the table below the keywords are shown in categories:

Category	Keyword
The Snowden case	NSA Monitoring Snowden PRISM
Acting "dark" on the internet	Tor Tails Web going dark How to hide something Peer to peer (P2P) Https
Firewall and antivirus	Firewall Antivirus
Encryption	Encryption Pretty Good Privacy (PGP)
Surveillance	Surveillance CIA
Other	Transparency Social engineering

In the Google Trends section is a detailed explanation of the method used to calculate the values for the search terms.

Uncertainties in search terms

Taking "Surveillance" as an example, the following will supply an overview of the uncertainties in relation to using search-numbers as data. When people are googling surveillance, it is given that information seek-

ing in this keyword to some degree is the goal but the actual relation is unknown. By this means the connection of surveillance in the search can be different but when looking into the time period of the Google Trend “surveillance” it could be argued that people around the world have a little interest in this.

By extension of that, an important question appears which is also situated in the analysis of the results and hereby the data seen from Google Trend. Do more searches for a topic mean a bigger awareness of that topic? It is not clearly a matter of course but at the same time, it might have some influence because Google as search engine has become a huge information source. When someone wants to find out something, Google may be first-of-mind in vast majority of people who are online.

Credibility

In order to ensure some credibility from this thesis, it is important to state to what degree the validity and reliability is seen. This is done by specifying the individual areas of the study which have influence to these sections individually. Respectively validity and reliability is covered in separate sections below.

Validity

Validity of a study states whether the study is usable and thereby whether it can be defined as “strength and valid”.³⁹ The validity of this thesis is of course with high priority because of the importance in having the study as being creditable. Seen from the other side, it is also important to be able to see the points of a study which have an impact on the validity. The validity is seen in many aspects of the paper which will be affected through the process of working with the paper. One important focus in constructing a high validity is on exposing and reducing any subjectivity. By having concrete examples related to these aspects, some decreasing factors from the study could be mentioned. Firstly, the fact that a case study is conducted in this thesis, which means the process of finding relevant literature by default is of a very subjectively character and this could create a tunnel-vision. This could be argued to create a lower validity because of the subjectivity but also from the point of seen every material from the case’s point of view every time a search is made. Though, it also ensures targeted searching for the specific topic which, all others being equal, would create a more complete knowledge for the topic, but this is not given as a positive thing in this relation.

³⁹ Kvale, Steiner & Brinkmann, Svend. (2011) *Interview*. 2. edition. P. 353

Another aspect which could argue to have a negatively impact on the validity, is the fact that the world is ongoing and many events occurring constantly. By looking at specific dates of changes in searching behaviour and use of privacy tools, there are not any circumstances which ensure that others events would not impact the results. To some degree, this could be argued to have only a minor effect, because big events such as the Snowden leaks are shown the media and besides this, it would only be such big events which could have a visualizing impact on the results.

Another important factor which is present in relation to validity, is the whole aspect of spelling correctly and meaning the same thing when searching for something by the users of Googles search engine. When results from Google Trends are collected, it is a matter of course that people spell these search terms correctly and are using the exact same words when searching, because any misspellings, abbreviations or synonyms are not present in the output of Google Trends. This could have an impact on the validity because not every search is present in the result then. It could though be argued that Google are very good at giving suggestions and correct misspellings, and this therefore are of minor impact.

Relating to the misspelling, it could even be synonyms for whole other topics, which would give false positives in the results. The search term "Tails" are a great example of this, because it has two meanings which are far from each other. This does definitely have an impact on the result, but to what degree, is hard to say. It is mentioned in the specific cases when this is suspected and seen in relation to the final conclusion, this is not the turning point.

The validity is increased because several graphs of the use of privacy tools. One or two could have been relatively selective chosen or could just have been coincidental in any changes of use. There is no magic by the number "3" but several graphs of the use of privacy tools combined with searching results, does have a better background for concluding something. Especially if these independent tools and searches are showing something unanimous.

A last aspect of validity is seen in the raw numbers from the results. The numbers speak for itself and no results are taking out which means a very broad perspective is seen in all of the results. If any interviews were made for supporting the results, it would both give concrete examples and it would be possible to deep into questions but it would also be very narrowed onto few respondents. The situation of personal contact could also have impact on the results if the respondent has issues to personal contact or something alike, but most important, the result would be subjectively interpreted. This is eliminated from the objective collection of raw numbers in this study. It could be further argued that this study has saturation of data because the comprehensive collection in the subject area from one of the world's biggest engines (Google) plus numbers from DuckDuckGo, Tor and Tails (see section "Results").

Reliability

The reliability lies in the way it is possible for a researcher to repeat the study at a different time and getting the same results from the same methodology and under the same conditions.⁴⁰ Reliability is not by default following the degree of validity, meaning the validity can be high and the reliability low, and the other ways around.

Conducting a totally similar study to an existing one is not easy but even though, this study does have a relatively high degree of reliability because almost no subjective involvement has been made. The only clear observable point of having directly subjective involvement is seen in the analysis and discussion, which is a matter of course. As examples of increasing the degree of reliability is seen from the ability of being able to obtain the same results in this particular study because the collected data are directly obtainable for everyone which relates to the core of reliability. This is further the grounding basis for the subjectively analysis and discussion from the results. Self-evident are this analysis and the discussions not able to be recreated but neither an important point of recreating the same conclusion. It would here be essential that the reliability must be individually assessed, and from this perspective, the individual must be able to calculate their own degree of reliability. It is important to state that the aspect of subjective discussions performed, are definitely not unusual and the estimation of reliability must thereby primarily rely on the data collection.

There are no clear observable points of lowering the reliability and from these points, the reliability must be considered as relatively high in this thesis.

⁴⁰ Kvale, Steiner & Brinkmann, Svend. (2011) *Interview*. 2. edition. P. 352

Results

From the previous chapter, it is now clear how and what to collect data about. In this chapter, the data collected and the parameters behind will be explained for further analyzing and discussing later.

The primary data collection tool used “Google Trends” and the process of collecting the data is elaborated on below. Furthermore, the actual results are visually outlined and described.

Google Trends

Google Trends makes it possible to collect data about specific searches performed by people all over the world. It is a tool based on searches performed in the well-known search engine, www.google.com.

Google Trends makes it easy to visualize trends in internet searches, hinting at hypes and concerns because it shows what people care about and therefore search for on google.com.

The results from Google Trends have the following settings in common, unless otherwise stated under each result:

- The search term “Tropical depression 9” has been used as a constant search term
- “Worldwide” was selected as the geographical area of interest.
- The custom time range of “2013-03-01 – 2016-08-03”.
- The category was set to “All categories”.
- The search type was set to “Web search”

The examined period for each graph is “2013-06-02 – 2013-06-08” unless otherwise stated under each result.

The constant search term is used to be able to estimate an approximate value to apply to the results, since Google Trends only supplies graphs where the highest value is set to 100%. This value is called **comparison value** in the following.

The comparison value 20.000+ was found on the date 2016-08-30 as one of the ‘Trending Searches’ of the day. When looking at search graphs they are pictured in percentages where the max value is set to 100%. Therefore, the comparison value is read in percentage and is called **comparison percentage** in the following.

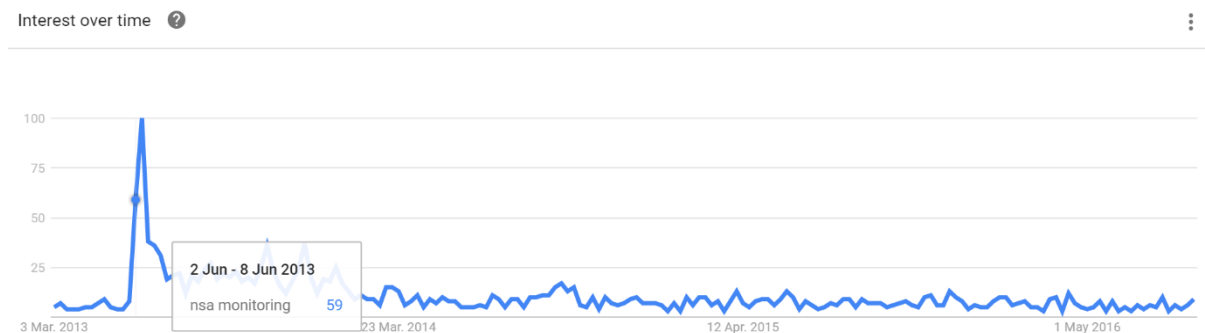
In the same way the value for the search term is read from the graph in percentage; in the following called **search term percentage**.

This leads to the calculation used for each keyword:

Average daily searches in the examined period = [Comparison value] / [Comparison percentage on 2016-08-30] * [Search term percentage at examined period]

Search Term: NSA monitoring

When looking up the trend of searching for “NSA monitoring” in Google Trends, there is a clear peak in the interest in this search term:



41

The highest number of searches can be found a few days after the case of Snowden as seen above. The problem of seeing the actual trend of this keyword lies in the scaling. When putting in another keyword the case is slightly different:



42

Because we know an approximate number of searches for “Tropical Depression 9” (red line) in the period of August 28, 2016 to September 3, 2016 which are 20,000+, it is possible to get a roughly number of searches for “NSA monitoring”. The 20,000 searches are the highest point reached in the right of the

⁴¹ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=NSA%20monitoring> – 2016-08-31

⁴² <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=NSA%20monitoring,Tropical%20Depression%209> – 2016-08-31

graph and therefore at 100%. When looking more into the little increasing in the period of the Snowden revelations, it shows a relative number of “2” as seen below.



42

Trend = In this graph it is clear that the trend of “NSA monitoring” is still highest (blue line) in the period around the Snowden case, but the absolute numbers are very low.

Comparison percentage on 2016-08-30 = 100

Search term percentage at examined period = 2

Average daily searches in the examined period = 400+

Search Term: Tor



43

Trend = Stagnating in the whole period with minor peaks all the time

Comparison percentage on 2016-08-30 = 11

Search term percentage at examined period = 66

Average daily searches in the examined period = 120,000+

⁴³ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Tor,Tropical%20Depression%209> – 2016-08-31

Search Term: Firewall

Interest over time ?



Trend = Slightly decreasing with small peaks and downwards different places back in time

Comparison percentage on 2016-08-30 = 31

Search term percentage at examined period = 91

Average daily searches in the examined period = 58,000+

Search Term: Snowden

Interest over time ?



Trend = A little delayed peak in interest followed by stagnation.

Comparison percentage on 2016-08-30 = 6

Search term percentage at examined period = 1

Average daily searches in the examined period = 3,300+

The peak is a few days later which is shown below:

⁴⁴ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Firewall,Tropical%20Depression%209> – 2016-08-31

⁴⁵ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Snowden,Tropical%20Depression%209> – 2016-09-01

Interest over time ?



Examined period = 2013-06-23 – 2013-06-29

Trend = After the peak, the interest is downward sloping where after few increases in peaks occur at several points.

Comparison percentage on 2016-08-30 = 6

Search term percentage at examined period = 1

Average daily searches in the examined period = 3,300+

Search Term: Encryption

Interest over time ?



46

Trend = No significant increase in the period of the Snowden leaks. The line is almost regular the whole period besides one big peak which must be related to another event.

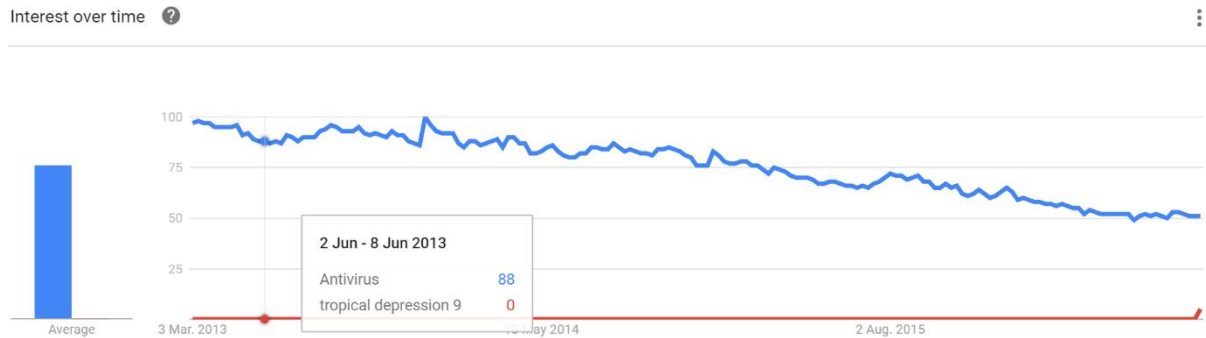
Comparison percentage on 2016-08-30 = 23

Search term percentage at examined period = 25

Average daily searches in the examined period = 21,700+

⁴⁶ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Encryption,tropical%20depression%209> – 2016-09-01

Search Term: Antivirus



47

Trend = Downward sloping with small peaks the whole period.

Comparison percentage on 2016-08-30 = 5

Search term percentage at examined period = 88

Average daily searches in the examined period = 352,000+

Search Term: Pretty Good Privacy



48

Trend = Almost complete stagnation throughout the period. Even though it has a little upward slope in the days after the Snowden leaks, in actual numbers of searches the rise is not that spectacular.

Comparison percentage on 2016-08-30 = 100

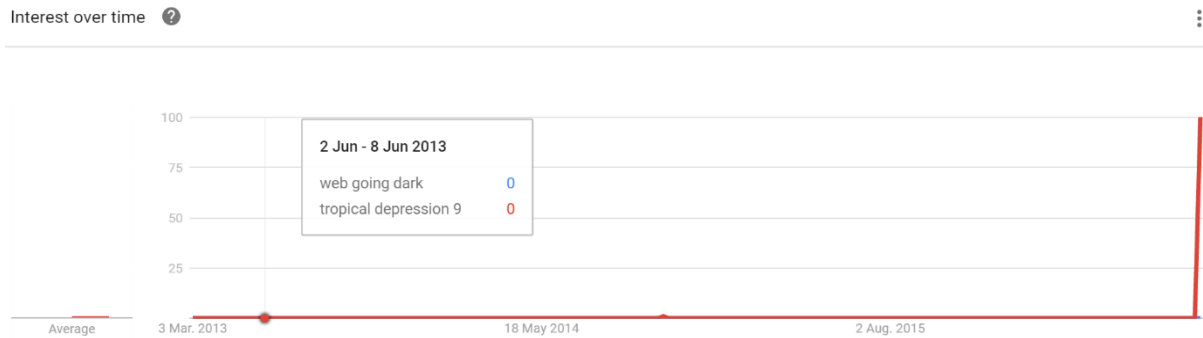
Search term percentage at examined period = 41

Average daily searches in the examined period = 8,200+

⁴⁷ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Antivirus,tropical%20depression%209> – 2016-09-01

⁴⁸ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=%2Fm%2F05rhl,tropical%20depression%209> – 2016-09-01

Search Term: Web going dark



49

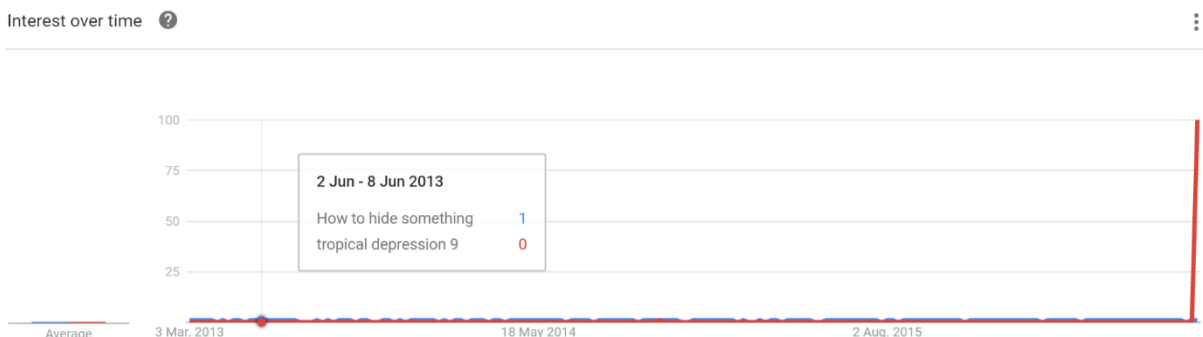
Trend = Below 1 and therefore shown as 0 the whole period (Google decides to show 0 when the number is below 1).

Comparison percentage on 2016-08-30 = N/A

Search term percentage at examined period = 0

Average daily searches in the examined period = 0

Search Term: How to hide something



50

Trend = The search term is of course broad in the sense that it is only the exact combination of the words which will be displayed in the result above and something to hide can be related to other aspects and create false positives. Nevertheless, it shows insignificant interest in this combination of words in the period of the Snowden leaks.

⁴⁹ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=web%20going%20dark,tropical%20depression%209-2016-09-01>

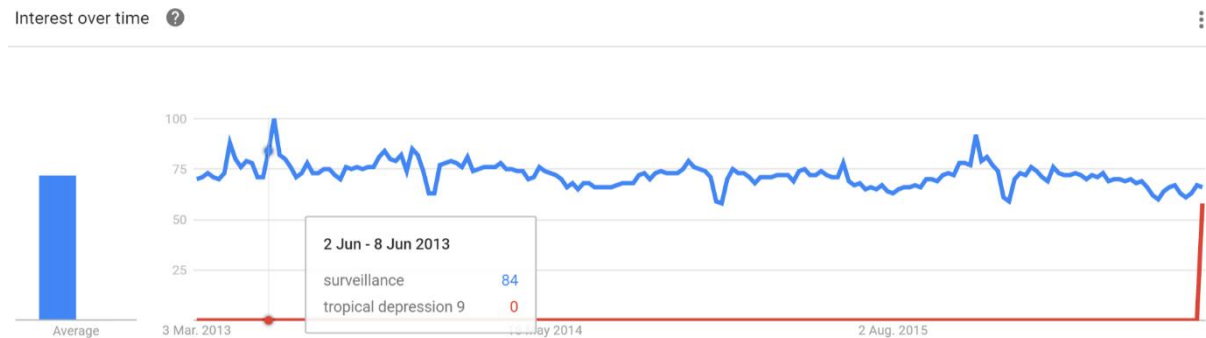
⁵⁰ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=how%20to%20hide%20something,tropical%20depression%209-2016-09-01>

Comparison percentage on 2016-08-30 = 100

Search term percentage at examined period = 1

Average daily searches in the examined period = 200+

Search Term: Surveillance



51

Trend = “Surveillance” is a topic which is relatively popular during the whole period with small peaks in several places. One slightly bigger peak after Snowden.

Comparison percentage on 2016-08-30 = 58

Search term percentage at examined period = 84

Average daily searches in the examined period = 28,900+

Search Term: Transparency



52

Trend = The trend of “transparency” is also broad because it can be seen in other aspects and hence include false positives. Significant spikes are seen throughout the period where transparent related events

⁵¹ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=surveillance,tropical%20depression%209> – 2016-09-01

⁵² <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=transparency,tropical%20depression%209> – 2016-09-01

are probably occurring.

Comparison percentage on 2016-08-30 = 91

Search term percentage at examined period = 52

Average daily searches in the examined period = 11,400+

Search Term: Https



53

Trend = Upward going for a time after the case of Snowden where it also has the biggest peak with the number of 100 from 90+ until almost a year later. Thereafter the trend is falling to an almost stabilizing level of 50 with only one big spike. This may be due to a broader use of https by major service providers lately.

Comparison percentage on 2016-08-30 = 15

Search term percentage at examined period = 54

Average daily searches in the examined period = 72,000+

⁵³ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=https,tropical%20depression%209> – 2016-09-01

Search Term: Tails

Interest over time ?



54

Trend = The trend of “Tails” have a lot of spikes throughout the period but not immediately following the Snowden leaks. Of course, there is also a risk of false positives with this search term, because “tails” has other usages besides as a security tool.

Comparison percentage on 2016-08-30 = 35

Search term percentage at examined period = 65

Average daily searches in the examined period = 37,100+

Search Term: Social engineering

Interest over time ?



55

Trend = Not very popular as a search term.

Comparison percentage on 2016-08-30 = 100

Search term percentage at examined period = 8

Average daily searches in the examined period = 1,600+

⁵⁴ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Tails,tropical%20depression%209> – 2016-09-01

⁵⁵ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=social%20engineering,tropical%20depression%209> – 2016-09-01

Search Term: P2P

Interest over time ?



56

Trend = In general a search topic which holds an interest with people. Many small and some bigger spikes throughout the whole period. The slope is going downward after the Snowden leaks.

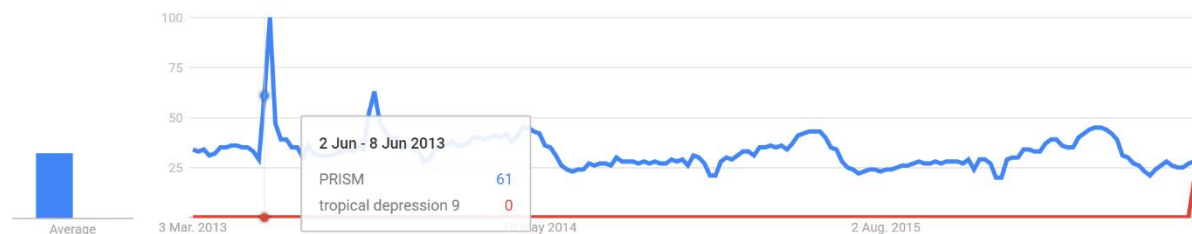
Comparison percentage on 2016-08-30 = 74

Search term percentage at examined period = 63

Average daily searches in the examined period = 17,000+

Search Term: PRISM

Interest over time ?



57

Trend = "PRISM", being a very targeted search term, should rule out false positives. The line has a clear spike in the period of Snowden.

Comparison percentage on 2016-08-30 = 18

Search term percentage at examined period = 61

Average daily searches in the examined period = 67,700+

⁵⁶ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=p2p,tropical%20depression%209> – 2016-09-01

⁵⁷ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=PRISM,tropical%20depression%209> – 2016-09-01

Search Term: CIA

Interest over time ?



58

Trend = “CIA” is clearly not a search term people have related to Snowden. This is probably to be expected, since CIA was not directly relevant to the Snowden case.

Comparison percentage on 2016-08-30 = 12

Search term percentage at examined period = 53

Average daily searches in the examined period = 88,300+

Privacy tools

Many people are not interested in being monitored while searching, and to this end, several open-source privacy tools have been created. Some of the biggest ones are briefly covered below, but many other methods/tools for staying anonymous exist.

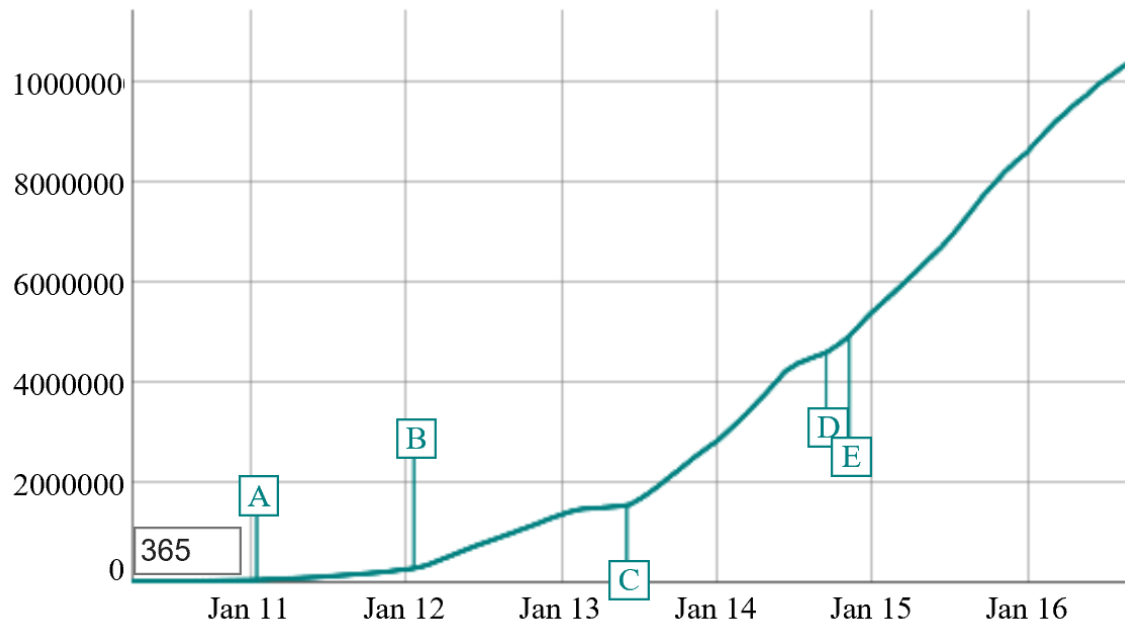
DuckDuckGo

DuckDuckGo is a search engine like Google, Bing, Yahoo etc. A clear difference, though, lies in the fundamental ideas behind its development. Unlike Google and the other major search engines, DuckDuckGo has a policy of not collecting personal information.

The number of searches done on DuckDuckGo has increased considerably through time as seen in the graph below. It should be pointed out that the number on the left side shows the number of queries made on the search engine and the highest number miss a 0 in the end and should be 10,000,000.

⁵⁸ <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=cia,tropical%20depression%209> – 2016-09-01

DuckDuckGo Direct queries per day (1y avg)



59

In the graph, several events are shown. These represent individual events which are relevant to the increase in use of DuckDuckGo through time. These are all further described in the table below:

Letter	Description
A	DuckDuckGo put a billboard up in San Francisco proclaiming: "Google Tracks You. We Don't" ⁶⁰
B	Google changed their privacy policy, allowing linkage of data from several products to the individual person. ⁶¹
C	The case of Snowden and the surveillance leaks occur. ⁶²
D	DuckDuckGo becomes a built-in search option in Safari. ⁶³
E	DuckDuckGo becomes a pre-installed search option in Firefox. ⁶⁴

59

⁵⁹ <https://duckduckgo.com/traffic.html> - 2016-08-30

⁶⁰ <http://www.wired.com/2011/01/duckduckgo-google-privacy/> - 2016-08-30

⁶¹ https://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQA8w8GOQ_story.html - 2016-08-30

⁶² <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/6> - 2016-08-30

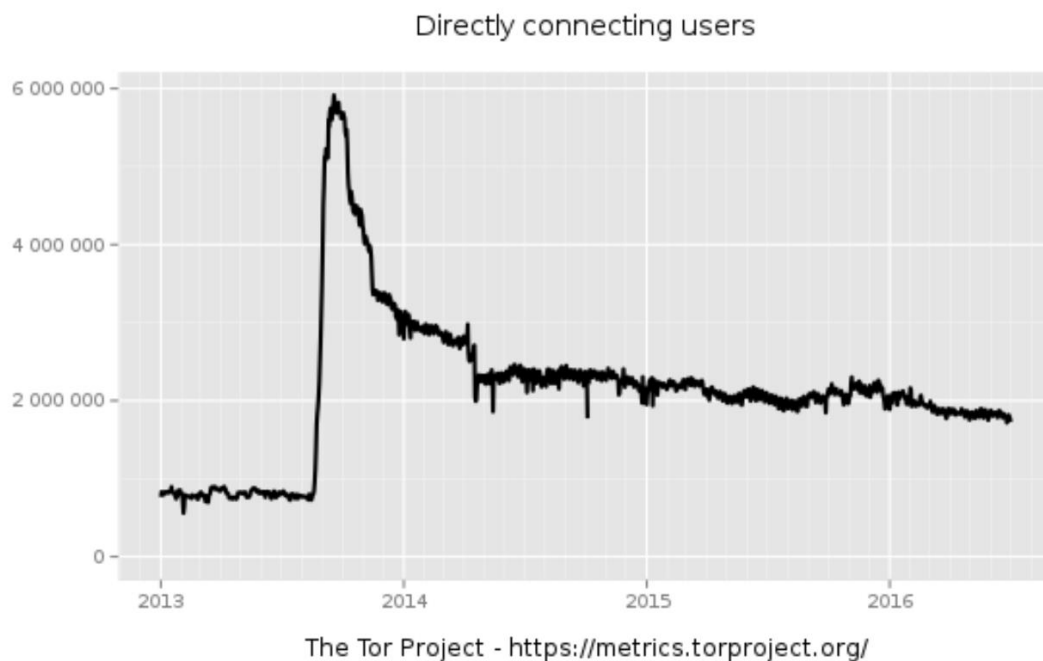
⁶³ <https://duck.co/blog/post/89/safari> - 2016-08-30

⁶⁴ <https://duck.co/blog/post/126/firefox> - 2016-08-30

Tor

Tor is a strong tool for securing privacy. It helps hiding its users through directing communication through an associated network. It was developed with the U.S. Navy in mind from the start. Besides this, Tor was designed, implemented, and deployed in a “third-generation onion routing project of the Naval Research Laboratory”. It was initially developed to secure government communication and is used by many people and organizations today, including the military.⁶⁵

The use of Tor has been more widespread than it is today, but after all, it has more than doubled since 2013:



Start date (yyyy-mm-dd):

End date (yyyy-mm-dd):

66

SecureDrop

SecureDrop is a part of Tor and describes themselves:

⁶⁵ <https://www.torproject.org/about/torusers.html.en> - 2016-09-01

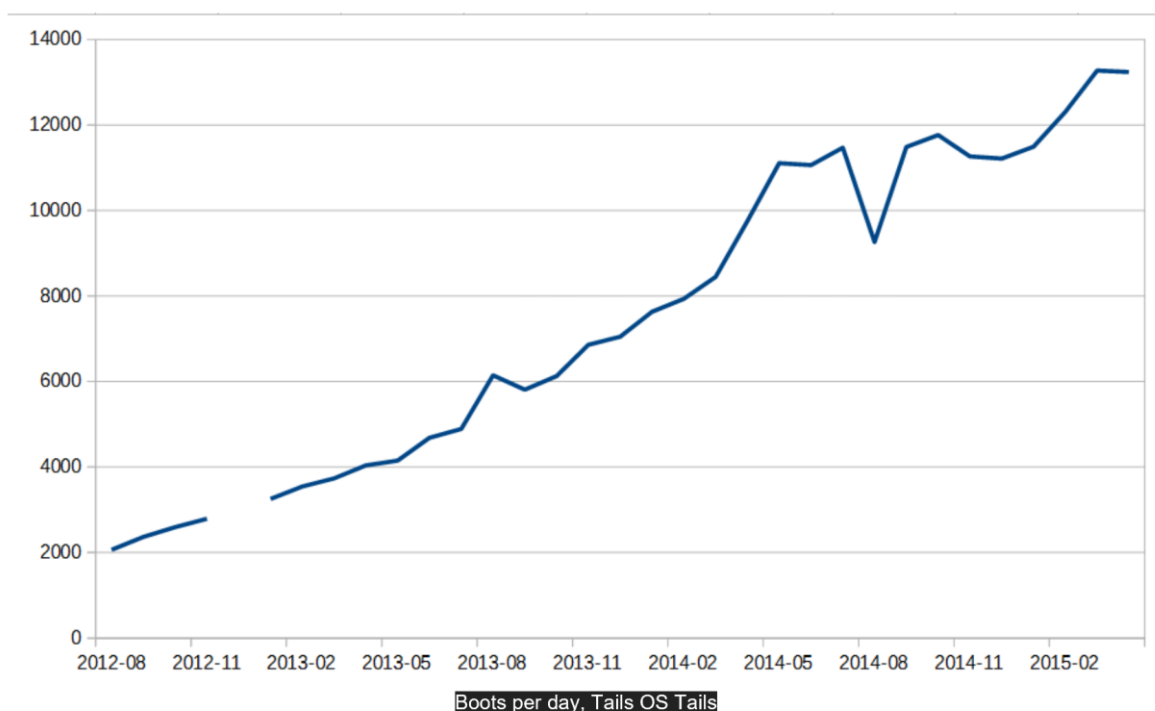
⁶⁶ <https://metrics.torproject.org/userstats-relay-country.html?start=2013-01-01&end=2016-07-01&country=all&events=off> – 2016-09-01

“SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. It was originally created by the late Aaron Swartz and is currently managed by Freedom of the Press Foundation”⁶⁷

SecureDrop is used by over 20 organizations and was also used in the case of Snowden by The New Yorker⁶⁸ and is used by The Guardian today.⁶⁹

Tails

Tails is another tool for getting privacy. It is a live system which can be booted from a USB, DVD, SD card etc.⁷⁰ The number of boots per day has increased over time as seen in the graph below:



71

⁶⁷ <https://securedrop.org/> - 2016-09-01

⁶⁸ <https://www.wired.com/2015/11/securedrop-leak-tool-produces-a-massive-trove-of-prison-docs/> - 2016-09-01

⁶⁹ <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents> - 2016-09-01

⁷⁰ <https://tails.boum.org/> - 2016-09-01

⁷¹ <http://www.dailydot.com/layer8/encryption-since-snowden-trending-up/> - 2016-09-01

Analysis and discussion

In this chapter, the results will be elaborated upon, through analyzation and discussion. Also, the earlier outlined literature review and clarified concepts will be taken into the discussion where appropriate. This analysis and discussion will be based on the theories outlined in the theory section with the primary goal of answering the research question of this thesis.

There is a grey area between transparency and control...

A situation of an extreme transparency would eliminate this problem because everyone would have access to all data, but this would also create some other bigger issues. Though this extreme situation is naturally also unrealistic but conditions in that relation is seen in some aspects of the society of the western world. This has much to do with the fact that more and more becomes electronic and the existence of cross indexing which also contributes to this. This also means that data is floating because no one really knows who has what information about me as person. The aspect of control is not opposite from transparency and this is a great example of having super control following super transparency. Though, both of the concepts are scalable which means there are several points of control and transparency before calling the situation for “super”. This also apply for the extremes.

Transparency

Most would probably consider increased transparency a positive development. It is what makes it possible to e.g. help finding lost goods,⁷² getting direct and personalized advertisement,⁷³ tracking a person in order to save this person from a life-threatening situation,⁷⁴ getting location history to recall the location of a specific time.⁷⁵

Also, knowing why politicians made their decisions, and on what foundation would make understanding the policy easier. Knowing exactly what information Google has on each person and precisely what it will be used for and how, would make it easier to decide what to share with Google. Knowing exactly what news was chosen by gatekeepers and what was omitted, including the reasoning (was some chosen because of payment?), would make evaluation of the news more exact. If all data from all sensors and devices were made transparent, scientists would have an excellent basis for research.

⁷² <https://play.google.com/store/apps/details?id=com.alienmanfc6.wheresmyandroid&hl=da> - 2016-09-04

⁷³ <https://techliberation.com/2011/01/28/digital-sensors-darknets-hyper-transparency-the-future-of-privacy/> - 2016-09-04

⁷⁴ <http://www.seattlepi.com/local/article/Using-cell-phones-to-find-missing-persons-pushes-1272414.php> - 2016-09-04

⁷⁵ <https://myaccount.google.com/activitycontrols/location> - 2016-09-04

Some argue that anyone denying to share information is really denying others a chance to learn.

Something to hide?

Does an aversion against sharing indicate that people have something to hide or could it just be that people want to have some privacy? Few would probably like to have government-installed surveillance cameras and microphones in their own homes.

Even though some argue that “if you have nothing to hide, you should have nothing to fear”, not many would like to share personal information such as health information, economic information, political leaning, sexual orientation, crimes conducted etc. Many would fear for this kind of information to be exploited.

The media’s focus on negative stories limit the desire to share information, from a fear of biased stories. Keeping information close is a way of protecting oneself from the repercussions of a society possibly moving towards super transparency or even extreme transparency. This is of course an extreme and probably unrealistic scenario, because even if some would support this situation, others would not accept it.

Concerned about transparency?

Google Trends reveals a modest interest in the search term “Transparency”, and also shows no increase in the period of the Snowden case. A minor spike some time after the leaks is seen, but no particular event seems to have driven this.

Today, the internet provides excellent possibilities for increased transparency, and in a small way, moves us closer to super transparency and extreme transparency, but this also calls for some concern over e.g. the unconcerned manner some people’s postings on social media.

Leaks = transparency?

In recent years, we have seen leaks besides the Snowden leak, such as Panama paper⁷⁶, Bank of America Email Drop⁷⁷, Anonymous Takes Down HBGary Barr⁷⁷, Luxembourg tax files⁷⁶ and many others.

These leaks are often justified with a wish for transparency. The question is, to what extent, leaks, as we have seen them so far, qualify as transparency. As long as gatekeepers decide what parts of the leaks are published, only part of the picture is presented.

⁷⁶ <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers> - 2016-09-08

⁷⁷ <http://www.complex.com/pop-culture/2011/08/the-10-craziest-anonymous-hacks/> - 2016-09-08

Fear of missing out

The topics of “NSA monitoring”, “Snowden” and “PRISM” are all pointing directly towards or almost towards the leaks of Snowden and thereby the case of Snowden. This is also seen in the trends collected from Google Trends which are very similar tendencies. The only one which stands out a bit is “NSA monitoring” because of the relative low level of approximate actual number of searches. The overall trend is though still present of having a slightly increasing interest in the period of Snowden or just after the Snowden leaks. This increasing interest are almost disappearing low after a short period for especially the keywords of “NSA monitoring” and “Snowden” but still a very decreasing interest for the trend of “PRISM”. This gives arguments for sensing a short trending of interest for the case of Snowden by people all over the world. When this is seen in connection to peoples social need from the Maslow’s Hierarchy of Needs, it gives a clear identification of confirming a need of being able to discuss the case of Snowden with others for being able to be social and belongs to a group. From the model of Maslow, this means people have to fulfill physiological and safety needs before the social need is in place. As the search words are in English, it refers a lot to the western world which has a relatively high standard of living and thereby have these two needs fulfilled to a degree that they seek the next need of social relations/longings. The next step of googling a case such as Snowden, could be by finding out how to protect themselves against surveillance. This is earlier covered.

People are especially expressing themselves on social media which correlates with the need of social interaction with others from Maslow’s hierarchy of needs. The limit of what to share are moving along with how much one uses social media which means more and more are shared. This is consistent with the dissemination of social media platforms which has become very popular recent years. Even though, people are also concerned of others opinions and this could create a minor decreasing in the transparency of expressions. This could have a direct connection to the surveillance from the government which again could have a relation to the increasing use of privacy tools as earlier seen.

Control

Control can be viewed as transparency, except, the information cannot be seen by the “target”, but by another party.

Control. Who benefits?

Obvious examples of professions enjoying great benefits from surveillance are the police and intelligence agencies. Investigating crime with more possibilities for tracking and monitoring e.g. suspected persons

and with easier access to evidence is clearly an advantage. This is probably perceived as a benefit for most of society, because more criminals will be held accountable for their deeds.

When deciding the allowed degree of surveillance for these agencies, a balance is struck, which is a recurrent subject for discussion. If agencies did not have the right to track and monitor, they would have tough conditions.

In western societies the permissions of intelligence agencies are often regulated by legislation. Judging from people's interest in searching for "CIA" for example, illustrates the degree with which people care about such agencies. When looking at the specific search term of "CIA" it shows a general interest, with a single peak in the examined period.

A type of control with both positive and negative perspectives is the increasing use of monitoring as a basis for insurance. It is, at least initially, an advantage to the insurance company, that they can do better risk estimates, but this also means that for some customers, this will result in higher insurance premiums. In the longer term, making too precise estimates may ultimately remove the incentive for the "high risk" customers to take out insurance in the first place.

From an economic perspective, people are maximizing their own utility by default (see section "Rational choice theory") and this affects their decisions. When e.g. a government has to decide on who and what to monitor, they will, according to this theory, be naturally tempted to include e.g. political opponents and others, who might be a threat.

According to the Foucault interpretation of the Panopticon theory (see section "Foucault and Panopticon") there is a relationship between power systems and information for getting even more information. This may be seen as frightening when seeing the theory in relation to the business providers of services with personal information as payment because they would get much control. Concretely, it could be nearing a situation of super control or even extreme control because few or one entity would have complete control for all people and would know everything about anyone.

Information as monetary value

Basically data is the new oil, meaning information is very useful and represents a monetary value and this is used as never before as payment for many things. This value could be in the form of tracking history of a person's physical movements as payment for a service.

A concrete example could be the Google Maps service. People have a benefit from using the service for driving directions with all its features and for this, people give, amongst other information, physical locations as payment for this service. This is a simple trade with two parties valuing the received asset as more valuable than the one given, in accordance with the earlier point of everything having a price, as expressed by economist and Nobel Prize winner, Milton Friedman by saying: “there ain't no such thing as a free lunch”.⁷⁸ The idea of personal information as an actual monetary value, should imply that people would protect their information, as it is seen from the graphs of Tor, DuckDuckGo and Tails.

Developing a world of surveillance

Products and services are available for what seems to be free to use without any monetary payment involved. Examples of these products/services could be social media platforms, health apps, map services, and much more.

The incitement for the developers lies in the possibility of enriching the data they receive as payment for their services. Businesses such as Google have many different products with different purposes and the data they collect from these various services can be cross indexed, adding even more information.

Developing such services and having people use them, paying with personal data, might seem difficult. However, with more than one mobile phone for every person in the western world (see appendix 3) the potential is huge. Besides this many other devices are connected every day giving even more incentive to deliver products and services for this market (see appendix 4).

If the use of privacy tools such as DuckDuckGo, Tails and to some extent Tor (see section “Results”) will continue to rise, it could point in a direction of much more awareness in this topic, because overall increased use is seen. If more people will be more aware of privacy, the future could end up with less “free” services or even a choice of cash as payment from the providers.

(Mass) surveillance?

Mass surveillance is associated with much, from surveillance cameras via Google’s collection of data to the surveillance done by intelligence agencies.

There are many contradictory opinions about surveillance. When it is serving the majority, when it is bothersome and when it is violating people’s privacy.

⁷⁸ The Oxford Dictionary of American Quotations. Hugh Rawson, Margaret Miner. 2006. P. 208

Many people are in doubt about what to think. Is it OK to monitor people suspected of terror? – What about the monitoring of innocent people? And how should someone thinking of using existing legislation as an excuse to monitor political opponents or enemies be dealt with? – Some believe the best of people but others are more skeptical.

National Surveillance Agency?

The Snowden leak exposed the NSA's attempt at installing infectious malware on PCs all over the world enabling them to remotely activate e.g. integrated cameras and microphones for surveillance purposes. (In turn causing a trend of putting tape or plates for integrated cameras and microphones in electronic devices, even by e.g. the director of FBI⁷⁹ and Mark Zuckerberg⁸⁰ (see "Appendix 2 – Primitive privacy tools")).

The question is then if NSA actually now has access or if the case of Snowden created too much attention on surveillance to being able to monitor people through this method?

The numbers from the results for the search terms "NSA monitoring", "Snowden" and "PRISM", only show a short term interest in the subject.

Session logging

Governments around the world have different ways of monitoring. Some include session logging of citizens' movements on the web. The Danish government is planning to reintroduce session logging with the reason of improving the police's work of collecting evidence. This means that all actions performed on the internet by the population in Denmark would be logged and stored with same precision as telephone calls.

Earlier experience with session logging from 2007 to 2014 has showed a minimal benefit of using it as stated in the following:

"A government evaluation report from December 2012 could only point to a single case, involving web banking fraud on a minor scale, where Danish police had been able to use the data collected with session logging."⁸¹

How much is the logging worth then? The government of Denmark must give it some value since discussing it re-introduced and combined with other ways of monitoring, it probably gives value in e.g. a cross-

⁷⁹ <https://www.theguardian.com/world/2016/jun/06/surveillance-camera-laptop-smartphone-cover-tape> - 2016-09-08

⁸⁰ <http://www.businessinsider.com/facebook-ceo-mark-zuckerberg-puts-tape-over-his-laptop-camera-2016-6?r=US&IR=T&IR=T> – 2016-09-08

⁸¹ <https://edri.org/danish-government-plans-to-re-introduce-session-logging/> - 2016-09-08

indexing relation. One thing is for sure – many innocent people will be monitored and this is probably a contributing factor for the increasing number of privacy tools being developed and used. Examples could be DuckDuckGo, Tor, Tails etc. (see section “Results”).

Controlling the crowd

As mentioned, research concludes that the majority of people in USA agree that monitoring is OK when the monitored people are suspected for terror. This is probably related to the high focus terrorism has in the media, and it seems like politicians exploit this fear for terror, to gain acceptance for increasing surveillance.

One problem with mass surveillance is that politicians, as earlier touched upon, may be tempted to use the increased surveillance for other purposes and, for instance, exploit the possibility to have their political enemies or foes in general monitored. This moves society in a direction of a less constraining legislation when it comes to surveillance and thus gives more control to the governments in the western world and less freedom for the population.

This thinking is based on a general mistrust of politicians, due to several examples of discovering them lying and being less transparent than desired.

The big doubt stems from not knowing when someone is watching you. This is directly comparable to the theory of Panopticon (see section “Foucault and Panopticon”). Every person who is online or have a personal device leaves digital footprints which creates a big digital exhaust for every movement, whether this is online or just by using an electronic personal device such as a smartphone. Businesses such as Google are good at cross indexing this information and this gives an even greater total amount of information because even more uncollected information is assembled from the collected ones and this means an even greater digital exhaust of every person. Panopticon is overall defined by a prison with minimum resourced used at the same time of maximum of utility. A prison is by default ran by an entity which would be the government in this situation and seen in relation of today, it could figurative be argued that everyone is in prison. No matter what a person do online, it is monitored at least to some degree by an entity whether it would be by the government or a business such as Google, Facebook or Apple. There is a doubt about what the individual measure is used for and who/what entity knows what about every person. This is also directly described in the theory of Panopticon and the idea also relates to recent times seen in many concrete situations (see section “Foucault and Panopticon”).

The backlash to this is seen from the increasing use of privacy tools and to some degree searching results for privacy tools. This would point in the direction of people being tired of being watched and having doubt about whether any monitoring is being performed against them.

By having a few entities to monitor, this creates conditions in a direction of super control because few entities know everything or almost everything about almost everyone (see section “Introduction to new concepts”).

Whether the society could come even further and thereby get closer to the concept of extreme control would be scary seen from the crowd because it would be much alike a controlling state by having only one entity would have all information about everyone.

When discussing mass surveillance, a recurring point is that it does not balance the price of monitoring innocent people with the limited value practical use has shown. This conflicts with fundamental democratic values and point towards a society with super control.

Government in the extreme?

Countries such as North Korea are probably the closest we have to extreme control, with a very centralized decision-making authority, in this case the government.

In a situation with near-extreme control, it will probably be hard to get the truth, when e.g. examining the privacy awareness in the population, but the question is what the reality looks like?

Even if the concept of extreme control seems very unrealistic in the western world, it is still a fact that it something close to exists in some parts of the world, with North Korea being a good candidate for the title. Extreme control is probably most likely to be seen in dictatorships.

Looking back at Foucault and the theory of discipline and punish, it would mean the government would have the authority to implement rules stating surveillance and monitoring of every citizen.

This gives cause to look back at some of the earlier points of having session logging reintroduced in Denmark and doubt about using threat from terror as reason for surveillance. Are governments in the western world going towards more control with today's conflicts of terror and immigrants as reason for doing so? And to what extend are companies able to obtain the same degree of control? Some could argue the direction is going against more control to a few or one entity from the just mentioned examples. Seen from the business side, legislation is helping to prevent single businesses having too much control but from the view of the government as the controlling unit, it is a bit harder to state an exact direction.

The government has much influence on the legislation, but the fact that the politicians are chosen by the citizens, will have a preventing effect. Though, this could also be manipulated as seen in some countries with dictatorship as the form of government. Several privacy tools are used as never before as seen earlier and this could also be an appose against the control from the government because water always find its way.

Modern technology is probably the only reason why this is even remotely possible.

Business control in the extreme?

In principle, the control could be done by a private business, making it probably wider, in the sense that the control could be global, but without the possibility to support it with legislation.

Fortunately, businesses are regulated by governments and legislation, which reduces the risk of having businesses gaining something close to extreme control. Concrete examples of this could be seen when AT&T⁸² was forced by a court of law to split into two. Also, Microsoft was nearly forced to split due to their dominant position on the operating system market.^{83 84}

Gatekeepers

The media has big role as gatekeepers. Seen in relation to the Gatekeeping Theory, this means the media decides what is communicated to the audience and thereby with what viewpoint it should be present. This can sometimes turn a story into a big scandal even if the actual point of the story has very little impact or proportion for the receivers of the story.

Concerned about control?

When looking at the trends for all search terms for the period of the Snowden leaks, nothing really spectacular can be seen. Over a longer period of time, the number of searches are steady, except for some peaks around the Snowden leaks. This could point in a direction of a slim connection between the Snowden leaks and more awareness of protection in the sense of privacy.

If people are truly not worried about privacy, the foundations for control and even super control are present, and the need of protecting should be unnecessary. In reality, a high degree of control would most likely create a condition of paranoia for people who are viewed as “normal”, but this is not always a bad

⁸² http://wps.aw.com/aw_carltonper_modernio_4/21/5566/1425000.cw/content/index.html - 2016-09-10

⁸³ <https://www.theguardian.com/technology/2000/jun/07/microsoft.business1> - 2016-09-10

⁸⁴ <http://time.com/3553242/microsoft-monopoly/> - 2016-09-10

thing as long as it does not get out of hand. Paul Bebbington (professor emeritus of mental health at University College London) puts this into words:

*"A little bit of paranoia might be quite helpful... When paranoid thoughts take over, it can be a mental disorder. But wariness and mistrust are not unusual... In fact, they're often protective, preventing people from, for example, blurting out their life's secrets to total strangers."*⁸⁵

Surveillance is used by both governments, private businesses and even private persons. The reasons vary but are often related to the entity having an interest in keeping track of the citizen or users' doings.

Steps like the Danish wish for session logging, point in a direction of governments working for more control by having the possibility to look into people's movements on the web.

This has created resistance movements and work against the increasing controlling conditions on several points. One such is "StopWatching.us"⁸⁶

Because some people are against conditions pointing in a direction of extreme control, several ways of getting around the logging exists by e.g. having VPN⁸⁷ or many tools for privacy which are covered in this thesis. This means the people who have something to hide does have possibilities of getting around the logging.

Privacy Tools

Sometimes people get frustrated enough over a situation, to seek tools for solving the concrete problem. This could be by sharing too much information from the digital exhaust to too many entities. From the results chapter above, the calculated approximate actual numbers are numbers of searches on Google. This means that people who are using other search engines to search for the same keywords, are not taking into account. The big question is then: "How many are this? – In what scale are we talking about?"

The point of, what is categorized as "the dark web", is to be anonymous to some degree and therefore it is not easy to clarify. Though, it is possible to look into the numbers of searches for this on Google. This would specify the searches for people interested in this, but only single searches would probably be found on every person, if we take for given that people search for it and thereafter use the tools they have searched for.

⁸⁵ <http://www.livescience.com/37419-paranoid-beliefs-common.html> - 2016-09-06

⁸⁶ <https://rally.stopwatching.us/> - 2016-09-04

⁸⁷ <https://www.expressvpn.com/what-is-vpn/logless-vpn> - 2016-09-08

Looking at concrete search terms from Google Trends for “Tor”, “Pretty Good Privacy”, “How to hide something”, “Https”, “Tails”, “Peer to peer/P2P” and “Web going dark” some interesting findings are seen for some of them. The search terms of “Tails”, “How to hide something” and “Web going dark” are almost imperceptible or totally unchanged in the period of Snowden. Though, with small peaks later in the full time period for “Tails” which could be based on false positives or a general base of interest for “Tails” through time.

When looking at the keywords of securing oneself or hiding searches from the provider “Tor”, “PGP” and “P2P” it is shown that a little spike is seen in the period of the leaks of Snowden or just after. This could look like a small or almost no changed awareness for people after the Snowden leaks but still a general interest in “Tor” since the approximate actual searches are relatively high in the period of the Snowden case (120.000+) and through the whole time period. Tor is software for anonymous communication and hide both the identity and location and this means people are general interested in privacy but not especially after the Snowden case.

Especially taking the before mentioned into consideration of single search from most persons, it may be seen as a relatively interesting topic through time. One thing is the interest for searching for it, but another thing is the actual use of Tor. This is one thing which is transparent for everybody to see and from here the actual numbers of connecting users are shown from back to the Snowden case to now (see section “Results”). From this graph there is a very clear increasing after the Snowden leaks which is actual numbers are approx. 1m to 6m in very short time. This increasing could easily be seen as a clear sign of more awareness of privacy. Whether it has something to do with the Snowden leaks is hard to say, but the time period of the increasing numbers is very close to the leaks by Snowden. Though, it is again the same picture of missing interest after a certain time, but overall the number of connections are steady at 2m which is an increase of 100% from the 1m before Snowden. This is still a noticeable sustained total increase although the decline has also been drastically.

For being secure of unwanted hackings and leaks, several methods and tools are used. When looking at the searches which have a connection to the ability to protect yourself, the following search terms are relevant: “firewall”, “antivirus” and “encryption”. These trends are interesting because both “firewall” and “antivirus” are downward sloping and “encryption” are stagnating with one peak years after the Snowden leaks. This means a decreasing or stagnating interest of these topics related to number of searches for these search terms which could be based on several reasons.

Are people protecting themselves less or could it be, that people already have protection? If people already have protection and are satisfied with the one they already have, they would just keep updating/buying license to this, and then it would create less interest for googling alternatives. An alternative is that people are tired of the crying wolf and therefore give up trying to protect themselves. This would also be consistent with the “nothing to hide” philosophy described earlier.

Contributing to support the idea about more awareness of privacy after the Snowden case, are both the trend of DuckDuckGo and Tails similar (see section “Results”). Both of them with an increase of use after the leaks of Snowden. Both graphs have an increase just after Snowden and have ever since been increasing. Being critical to these increases, it could also be argued that it is a coincidence or a trend which have been spread by mouth to mouth instead of from the Snowden case. If this were the case, this would then argue for the falling trend of Tor after a certain time.

Going back to the search terms from Google Trends, the search term “Https” stands out a bit because it has almost no change in the period of the Snowden case but a little time after, a big increasing which also have the biggest peak in the whole period. This increasing keeps going on for approximate a year and after this peak, the grounding point stays at 50 (approx. 120,000+ searches). This indicate a general interest with an even bigger interest before. “Https” is a very specific keyword and it is therefore reasonably certain that searches for this is targeted this specific search term which could point in a direction of more awareness of having secured webpages. Because Https is a protocol for secure communication, is would be tempting to state that most of the searches are performed in a business view to find out how to secure a webpage for the customers visiting the page.

On the other side, it could also indicate that people care more about the webpages they are visiting and therefore want to know what https is, or how it works. One of the ground reasons for implementing the https protocol, is namely to secure the identity and thereby not share any personal information. Sharing information is though more ongoing than ever and the limitation of what is acceptable for different persons to share can vary and the knowledge about what is given as quid pro quo for a service is not always clear defined.

The question is whether the primary reason for using these tools are intentionally based on the fact that the information has a monetary value or it is more related to the intention of keeping some privacy? One thing is for sure, the value of information is present and this value is tradable for assets which gives many possibilities which is a whole new way of see data and the possibilities in this. But it also means that people have something of value which would be tempting to get in possession of for thieves.

Conclusion

This thesis was built on an expectation that the Snowden case would have raised the bar, regarding people's awareness on privacy. This is reflected in the research question of the paper, which is answered below. Through the data collection and analysis and discussion, it was shown that this expectation was not fulfilled. The work on this thesis, has brought the following conclusions as results of the research.

The awareness of privacy concerns in relation to surveillance did not in general rise significantly due to the Snowden leaks when looking at Google Trends of specific search words. Only search terms related to the case was having a slightly increasing with a decrease short after and small peaks in the interest in terms of searches. This interest may be partially a question of people's need to have social interaction and the need of safety. It is also concluded that the use of Google Trends works well for identifying variations, but is not suitable for providing absolute numbers for searches.

Another conclusion is seen in the use of privacy tools which have seen a relatively steep increase after the Snowden leaks. Though, it is still not very significant in absolute numbers but still clear to see an actual increasing of use. Specially in the use of DuckDuckGo and Tails whereas Tor was having a big increasing effect followed by a decreasing short after the period of Snowden. This development could be attributed to the case of Snowden by having people more aware of privacy concerns related to surveillance.

When looking at the aspect of transparency from the research question, it is concluded that several information is public on the web and businesses are earning huge on these data. Data has becoming a monetary value which means people have a lot of opportunities to use services with personal information in return.

In relation to the insignificant awareness of privacy concerns, this can be a driver towards more control, since concern would work as a barrier against increased control. The Snowden case has a lot to do with the concept of control and it is concluded that several point of the society has a direction of more control whether it would be by surveillance or gatekeepers deciding what to be shared.

The concepts of transparency and control in its expanded version of this paper, has had much attention with especially control as the consistent theme. In this thesis these have been very interesting in relation to the case of Snowden and many aspects have been analyzed and discussed with the research question in focus.

Limitations of this research

In this section, the overall possible weakness and uncertainty of the thesis are described.

The first and possible most important point of limitations of this research is seen in the use of Google Trend and the lack of being able to have actual numbers of searches directly from the source of Google. This gives inaccurate actual numbers because approximate numbers are calculated. Google Trend is used for having an overall picture of specific keywords and thereby see the direction of these trends from the chosen periods. It could though have been resolved to some degree by downloading the accompanying CSV file because it would give the same numbers but from every day in the chosen period of 2013-03-01 to 2016-08-30. From this, own graphs and illustrations could have been created. This was though discovered too late in the process of the project to be done. The limitation does therefore lie in the opportunity to have more accurate illustrations but still not with actual numbers.

Further research

From the conducted thesis, there are potential for researching further in the overall topic of privacy awareness related to surveillance, transparency and control and the idea of the invented scalability of these.

The first view which could be very interesting to research further from this study, is based on the view from the increasing use of social media and thereby deep more into the data behind. People are expression much feelings and thoughts on social media and it would therefore be a great point of knowing people's awareness of certain topics. This could be done by using data collection tools such as Radian6 with possibilities to go back in time and look at keywords relating to the topic in this thesis. This is though expensive when using Radian6, but others could exist to this. Going this way, it could be a good starting point to look at the used keywords in this thesis to compare against the searches from Google Trends. To analyze these data and comparing them, the theory of "Spiral of silence" could be used with great advantage.

Another point which could extend the research in this thesis, is the use of other statistics of other privacy tools. This could again be analyzed and hold against the ones of DuckDuckGo, Tor and Tails seen in this thesis. It could also be discovered whether new privacy tools are developed and whether they have the same purpose of privacy on the web. It could also have a focus on whether new tools are developed with the purpose of securing other aspects of privacy from e.g. social engineering.

Also a whole business aspect could be made and thereby interviewing people from several businesses for researching whether they have an increasing focus on privacy, data loss, security or IT policies.

Besides this, it is earlier seen that an app as example seems like a tool for e.g. power saving, but instead were a monitoring tool. This could be covered by researching whether any tool is transparent and actually does what it states to do. This could also basically be a study of discovering whether people even are as "safe" as they think they are when using such privacy tools.

Another thing which could be very interesting to study is the detailed look of what information people are most likely and less likely to submit to third parties. And what service they would have as quid pro quo for delivering this personal information? Does people have any idea of what their data is worth and is this different from person to person? Does standard of living have a relation to this? Is it fair that any government are able to have almost any information about every citizen for free or should they buy them as

all others? These are all questions which could be examined from the case of Snowden or another event/case with surveillance or the new view of transparency and control in mind.

A last suggestion for further research is by looking at other cases and compare these and the impact of them to the one of Snowden. Still with the focus on the surveillance, transparency and control but also in relation to today, could be an idea.

Bibliography

Books

1. [1] Birkler, Jacob (2005). Videnskabsteori – en grundbog. Gyldendals bogklubber.
2. [1] Brickley A., James, Smith W. Clifford & Zimmerman L. Jerold. (2009 fifth edition) Managerial Economics and Organizational Architecture. McGraw-Hill Irwin
3. [1] Greenwald, Glenn. (2014) No place to hide – Edward Snowden, the NSA and Surveillance State.
4. [1] Gutting, Gary (2005). Foucault: A very short introduction. Chapter 8: Crime and punishment. Oxford University Press.
5. [1] Jacobsen, Dag Ingvar Jacobsen & Thorsvik, Jan (2008). Hvordan organisationer fungerer. Hans Reitzels Forlag.
6. [1] Kvale, Steiner & Brinkmann, Svend. (2011) Interview. 2. edition.
7. [1] Rienecker, Lotte and Jørgensen, Peter Stray (2011). Den gode opgave. Samfundslitteratur.
8. [1] Vøxted, S. (2006). Valg der skaber viden – om samfundsvidenskabelige metoder.
9. [1] Yin, Robert K (2009). Case Study Research – Design and Methods. SAGE Publications Inc.

Articles

1. [1] Asch, E., Solomon (1955). Opinions and Social Pressure. Scientific American
2. [1] Hampton, K.N., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). Social Media and the 'Spiral of Silence. Pew Research Center.
3. [1] Hodgson, M. Geoffrey. (2012) On the Limits of Rational Choice Theory. University of Hertfordshire Business School, UK
4. [1] Nahon, Karine. (2009). Gatekeeping: A critical review. Annual Review of Information Science and Technology.
5. [1] Noelle-Neumann, Elisabeth (1993). Spiral of silence. McGraw-Hill.
6. [1] Preibusch, Sören. (2015) Privacy Behaviors After Snowden. Communications of the ACM
7. [1] Rainie, Lee & Madden, Mary. (2015) Americans' Privacy Strategies Post-Snowden. Pew Research Center
8. [1] Roznowski, L. Jo Ann. (2003) A CONTENT ANALYSIS OF MASS MEDIA STORIES SURROUNDING THE CONSUMER PRIVACY ISSUE 1990-2001. Wiley InterScience.
9. [1] Stoycheff, Elizabeth (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. Journalism & Mass Communication Quarterly.

10. [1] The Oxford Dictionary of American Quotations. Hugh Rawson, Margaret Miner. 2006

Webpages and online articles

1. <http://www.internetociety.org/your-digital-footprint-matters> - 2016-07-16
2. [1] http://data.library.ubc.ca/guide/whats_difference.html - 2016-07-17
3. [1] <http://edition.cnn.com/2013/09/11/us/edward-snowden-fast-facts/> - 2016-07-10
4. [1] <http://gatekeepingtheory.weebly.com/> - 2016-08-25
5. [1] <http://media.greenmonk.net/greenmonk/files/2015/06/Screen-Shot-2015-06-16-at-19.44.18.png> - 2016-09-10
6. [1] <http://time.com/3553242/microsoft-monopoly/> - 2016-09-10
7. [1] http://wps.aw.com/aw_carltonper_modernio_4/21/5566/1425000.cw/content/index.html - 2016-09-10
8. [1] <http://www.bbc.com/news/magazine-23902918> - 2016-08-09
9. [1] <http://www.businessinsider.com/facebook-ceo-mark-zuckerberg-puts-tape-over-his-laptop-camera-2016-6?r=US&IR=T&IR=T> – 2016-09-08
10. [1] <http://www.businessinsider.com/facebook-ceo-mark-zuckerberg-puts-tape-over-his-laptop-camera-2016-6?r=US&IR=T&IR=T> – 2016-09-08
11. [1] <http://www.citi.io/2015/10/20/the-top-facts-figures-about-europes-e-commerce-2015/> - 2016-09-10
12. [1] <http://www.complex.com/pop-culture/2011/08/the-10-craziest-anonymous-hacks/> - 2016-09-08
13. [1] <http://www.csub.edu/~sledford/> (08-09-2016).
14. [1] <http://www.dailydot.com/layer8/encryption-since-snowden-trending-up/> - 2016-09-01
15. [1] <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#175b9ed334c6> – 2016-09-10
16. [1] <http://www.livescience.com/21569-deduction-vs-induction.html> - 2016-09-10
17. [1] <http://www.livescience.com/37419-paranoid-beliefs-common.html> - 2016-09-06
18. [1] <http://www.seattlepi.com/local/article/Using-cell-phones-to-find-missing-persons-pushes-1272414.php> - 2016-09-04
19. [1] <http://www.simplypsychology.org/maslow.html> - 2016-08-09
20. [1] <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/6> - 2016-08-30
21. [1] <http://www.wired.com/2011/01/duckduckgo-google-privacy/> - 2016-08-30

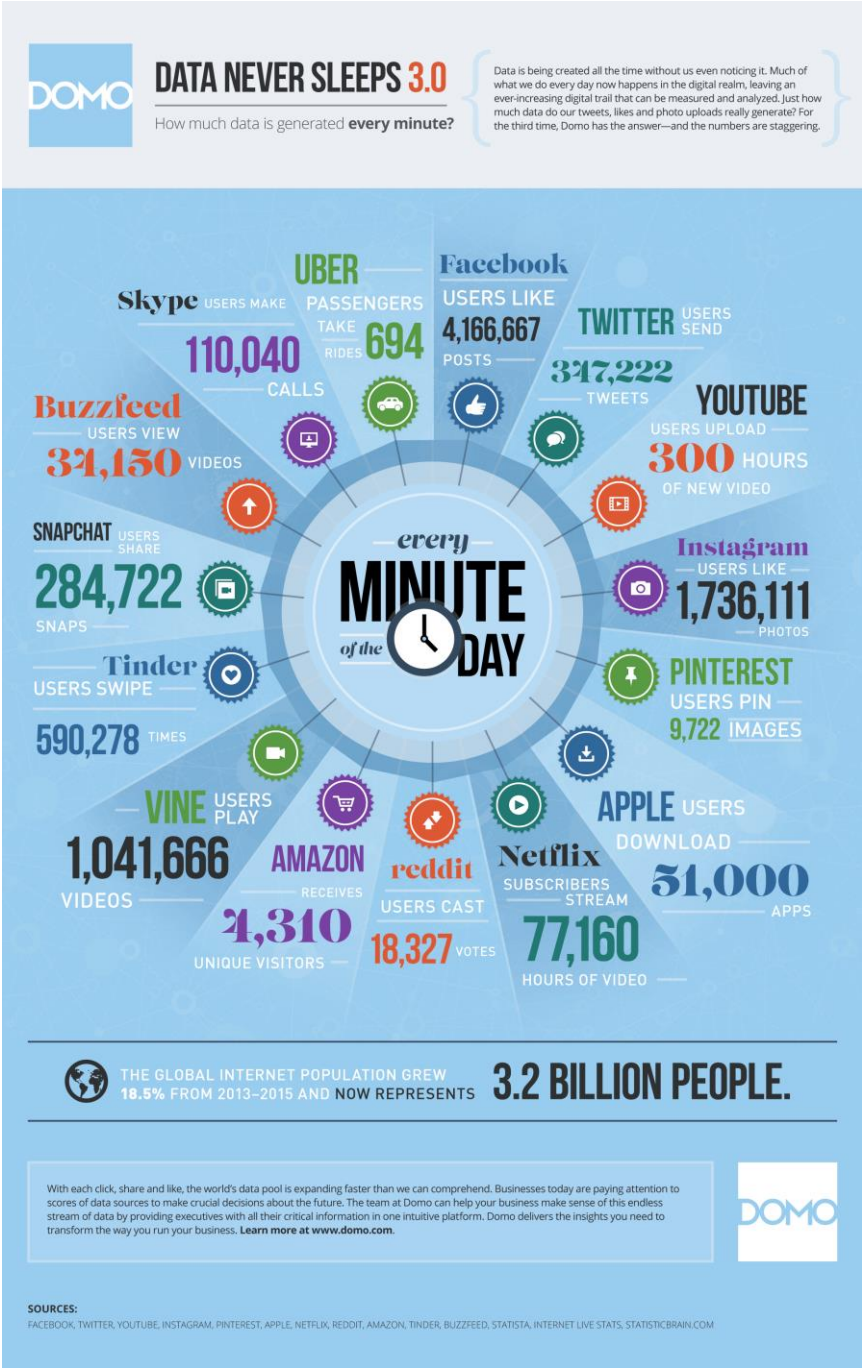
22. [1] <http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> - 2016-07-17
23. [1] <https://cpj.org/reports/2006/05/10-most-censored-countries.php> - 2016-07-20
24. [1] <https://duck.co/blog/post/126/firefox> - 2016-08-30
25. [1] <https://duck.co/blog/post/89/safari> - 2016-08-30
26. [1] <https://duckduckgo.com/traffic.html> - 2016-08-30
27. [1] <https://edri.org/danish-government-plans-to-re-introduce-session-logging/> - 2016-07-20
28. [1] <https://edri.org/danish-government-plans-to-re-introduce-session-logging/> - 2016-09-08
29. [1] <https://metrics.torproject.org/userstats-relay-country.html?start=2013-01-01&end=2016-07-01&country=all&events=off> – 2016-09-01
30. [1] <https://mic.com/articles/145220/this-is-why-you-might-want-to-put-a-strip-of-tape-on-your-laptop-camera#.ZlQQuH7mG> – 2016-09-08
31. [1] <https://myaccount.google.com/activitycontrols/location> - 2016-09-04
32. [1] <https://play.google.com/store/apps/details?id=com.alienmanfc6.wheresmyandroid&hl=da> - 2016-09-04
33. [1] <https://rally.stopwatching.us/> - 2016-09-04
34. [1] <https://securedrop.org/> - 2016-09-01
35. [1] <https://tails.boum.org/> - 2016-09-01
36. [1] <https://techliberation.com/2011/01/28/digital-sensors-darknets-hyper-transparency-the-future-of-privacy/> - 2016-09-04
37. [1] <https://www.comscore.com/Insights/Rankings/comScore-Releases-February-2016-US-Desktop-Search-Engine-Rankings> - 2016-07-21
38. [1] <https://www.domo.com/blog/2015/08/data-never-sleeps-3-0/> - 2016-07-20
39. [1] <https://www.domo.com/blog/2015/08/data-never-sleeps-3-0/> - 2016-07-20
40. [1] <https://www.expressvpn.com/what-is-vpn/logless-vpn> - 2016-09-08
41. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=%2Fm%2F05rhl,tropical%20depression%209> – 2016-09-01
42. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Antivirus,tropical%20depression%209> – 2016-09-01
43. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=cia,tropical%20depression%209> – 2016-09-01
44. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Encryption,tropical%20depression%209> – 2016-09-01

45. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Firewall,Tropical%20Depression%209> – 2016-08-31
46. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=how%20to%20hide%20something,tropical%20depression%209> – 2016-09-01
47. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=https,tropical%20depression%209> – 2016-09-01
48. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=NSA%20monitoring> – 2016-08-31
49. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=NSA%20monitoring,Tropical%20Depression%209> – 2016-08-31
50. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=p2p,tropical%20depression%209> – 2016-09-01
51. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=PRISM,tropical%20depression%209> – 2016-09-01
52. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Snowden,Tropical%20Depression%209> – 2016-09-01
53. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=social%20engineering,tropical%20depression%209> – 2016-09-01
54. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=surveillance,tropical%20depression%209> – 2016-09-01
55. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Tails,tropical%20depression%209> – 2016-09-01
56. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=Tor,Tropical%20Depression%209> – 2016-08-31
57. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=transparency,tropical%20depression%209> – 2016-09-01
58. [1] <https://www.google.com/trends/explore?date=2013-03-01%202016-08-30&q=web%20going%20dark,tropical%20depression%209> -2016-09-01
59. [1] <https://www.google.com/trends/hottrends> - 2016-09-03
60. [1] https://www.ics.uci.edu/community/news/articles/view_article?id=217 – 2016-08-20
61. [1] <https://www.privacyinternational.org/node/52> - 2016-09-10
62. [1] <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers> - 2016-09-08

63. [1] <https://www.theguardian.com/technology/2000/jun/07/microsoft.business1> - 2016-09-10
64. [1] <https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents> - 2016-09-01
65. [1] <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> - 2016-08-20
66. [1] <https://www.theguardian.com/world/2016/jun/06/surveillance-camera-laptop-smartphone-cover-tape> - 2016-09-08
67. [1] <https://www.torproject.org/about/torusers.html.en> - 2016-09-01
68. [1] <https://www.utwente.nl/cw/theorieenoverzicht/Theory%20Clusters/Media,%20Culture%20and%20Society/gatekeeping/> - 2016-08-25
69. [1] https://www.washingtonpost.com/business/technology/faq-googles-new-privacy-policy/2012/01/24/gIQAfw8GOQ_story.html - 2016-08-30
70. [1] https://www.whistleblower.org/snowden-timeline?gclid=Cj0KEQjwnv27BRC-muZqMg_Ddmt0BEiQAgeY1lxpkGQYwTF9sFwTUMDqQDJbeeA_XNlpKtLXq-mDmvpcaAsYf8P8HAQ – 2016-07-08
71. [1] <https://www.wired.com/2015/11/securedrop-leak-tool-produces-a-massive-trove-of-prison-docs/> - 2016-09-01

Appendixes

Appendix 1 – Data never sleeps




⁸⁸ <https://www.domo.com/blog/2015/08/data-never-sleeps-3-0/> - 2016-07-20

Appendix 2 – Primitive privacy tools






Family Pack (3) 1.0 Black
★★★★☆ 90
\$14.95 Prime



Webcam Cover
★★★★☆ 80
\$5.95

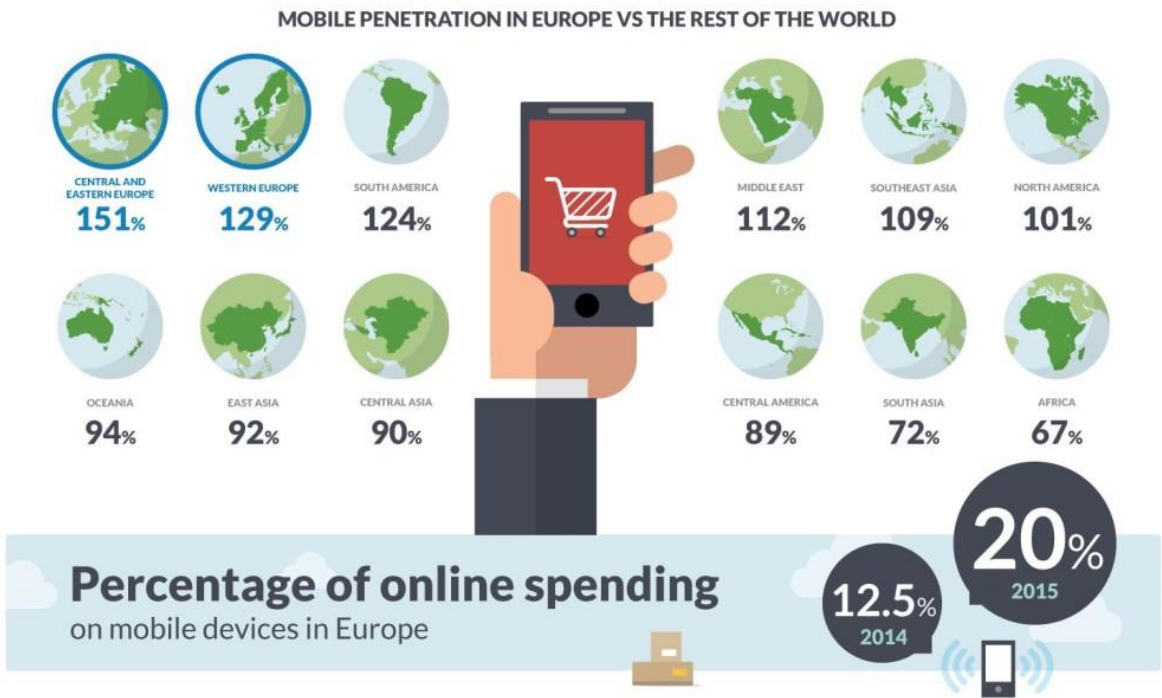


Webcam Cover for Laptops/Pad Devices
★★★★☆ 130
\$5.95

⁸⁹ <http://www.businessinsider.com/facebook-ceo-mark-zuckerberg-puts-tape-over-his-laptop-camera-2016-6?r=US&IR=T&IR=T> – 2016-09-08

⁹⁰ <https://mic.com/articles/145220/this-is-why-you-might-want-to-put-a-strip-of-tape-on-your-laptop-camera#.ZlQQuH7mG> – 2016-09-08

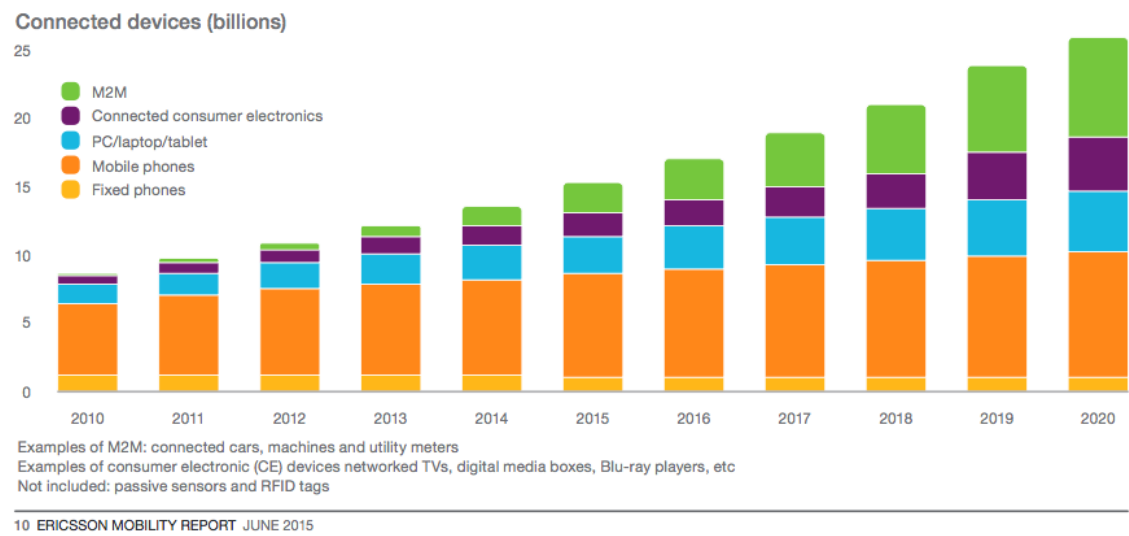
Appendix 3 – Mobile penetration globally



91

⁹¹ <http://www.citi.io/2015/10/20/the-top-facts-figures-about-europes-e-commerce-2015/> - 2016-09-10

Appendix 4 – Connected devices and future forecast



⁹² <http://media.greenmonk.net/greenmonk/files/2015/06/Screen-Shot-2015-06-16-at-19.44.18.png> - 2016-09-10