Utilitarian Analysis of Mass Surveillance: Panopticons and Privacy

M.Sc. (Tech) Thesis
UNIVERSITY OF TURKU
Networked Systems Security
July 2020
Muhammad Bilal

Supervisors:
Antti Hakkala
Jouni Isoaho

BISMILLA HIR-RAHMAN IRAHEEM
(By the name of ALLAH, the most Beneficent, the most Merciful)

Turun yliopisto
University of Turku

Ackowledgement

My acknowledgement forms a trinity primarily which includes my GOD (ALLAH), my parents and my teachers. Because all these three entities supported me unconditionally. I belong to a culture where teachers are considered as “Spiritual Parents” and here in Turun Yliopisto, every single teacher I came across really presented me the replica of my cultural belief. I would always be happy if I could ever be of any service to any of them. May all of them stay blessed, Amen.

UNIVERSITY OF TURKU
Department of Future Technologies

Muhammad Bilal: Utilitarian Analysis of Mass Surveillance: Panopticons and Privacy

M.Sc. (Tech) Thesis, 74 p., 2 app. p.
Networked Systems Security
July 2020

Utilitarian thinking comes under the wider framework of normative ethical theories which judges the morality of any act based on the outcomes achieved. Normative Ethics is the discipline of social sciences that comes under the head of philosophy which is based on moral principles. Based on such moral principles, any act is being considered as either right or wrong. Like any other domain, cyberspace also has some ethical values. To understand the ethics on Cyberspace, first we need to understand that how internet works and how many layers it has and what kind of activities are possible over every layer, respectively.

This thesis aims to explain the privacy issues caused by Panopticons related to illegal, unethical, and un-consensual mass surveillance across the internet via using various insidious methodologies. It also explains that who panopticons are and how this terminology came into existence and how it replicates current era's mass surveillance? Moreover, it addresses the parameters under which any surveilling authority could be declared as a Panopticon.

It explains that how and why Panopticons are doing unauthorized, unethical and non-consensual mass surveillance and how that surveillance actually takes place and up to which extent Panopticons have gone to achieve their desired mode of surveillance and it highlights different actors that are involved in mass surveillance at different scales via different techniques. The involvement of Governments with or without the collaboration of Private Internet companies has also been a shady topic exactly till Snowden made his revelations which later on caused a drastic awareness among masses and opened new doors of discussion as well as urged authorities to take some practical measures in order to curb the mass surveillance. That is why, Snowden's revelations have been taken as a case study to present the depth and techniques of mass surveillance that are in practice both by private and government organizations.

The analysis part holds the primary importance in this thesis, that's why the thesis concludes with analyzing ethical aspects of Mass Surveillance via Utilitarian point of view which analyzes the Snowden's act of reveling classified information and the corresponding top three accusations posed on him by USA's house of representatives, followed by legal and cultural implications.

Keywords: Panopticism/Panopticons, Mass surveillance, Snowden's Revelations, Utilitarian Analysis.

Table of Contents

Abbreviations and Acronyms

AI	Artificial Intelligence
API	Application Programing Interface
CCTV	Closed Circuit Television
CIA	Central Intelligence Agency
CSync	Cookies Synchronization
ECHR	European Convention of Human rights
EGE	European Group on Ethics (In Science and Technology)
FBI	Federal Bureau of Investigation
GCHQ	General Communication Head Quarters.
HTTP	Hypertext Transfer Protocol
HUMINT	Human Intelligence
IC	Intelligence Community
IC WPA	Intelligence Community Whistleblower Protection Act
IMINT	Imagery Intelligence
ISP	Internet Service Providers
LSO	Local Stored Objects
MASINT	Measurement and Signature Intelligence
NSA	National Security Agency
OSINT	Open Source Intelligence
PPD	Presidential Policy Directive
SIGINT	Signal Intelligence
SOCMINT	Social Media Intelligence
SOP	Same Origin Policy
SWF	Small Web Format
TOR	The Onion Router
URL	Uniform resource locator

List of Figures

Chapter 1: Introduction

Whenever any new technology is launched, people are less pragmatic and more excited in the beginning but gradually as time goes by, different issues compel the users towards pragmatism as well as towards further enhancement of such issues. Similarly, the norms set by any technology-oriented vendor initially are being accepted by masses right away without foreseeing the future concerns mostly even being pragmatic. And those standards related to any technology-oriented solution becomes a de-facto standard among general public because we are living in a fast-paced world where time is money so, people are mostly reluctant to wait for any kind of official standardization in terms of ethical dos and don'ts especially when it comes to technology. Similarly, such de-facto practices are appeared in case of internet as well. E.g. Most of the internet users agrees to terms and conditions of any website blindly without considering its after affects. Its just one example to define how things usually get accepted by public and then how such acceptance leads to the development of self-made norms which may or may not be ethical.

Much work has been done on the ethics but, within the rapidly changing technological advancements both on software as well as on hardware level, the need to update as well as modify the ethics always catches the attention of researchers and philosophers. Talking about internet and ethics is like discussing entirely a whole different universe floating over the networks solely. Due to which we need to narrow down our scope in terms of ethics under consideration. Therefore, this document will be focused on the issues caused by panopticons and mass surveillance that appears to be a threat to user privacy from ethical point of view.

The prevalent use of modern technology and internet has brought human beings at such a contemporary lifestyle where multiple gadgets being connected over the networks are controlling various routine life activities e.g. smart homes, smart grid stations, self-driving cars etc. Within the ease, there comes a responsibility of making sure the use of technology to be done in morally acceptable ways or to barrier human activities in this regard followed by a continuous monitoring as well as accountability. This documents implies ethical considerations regarding panopticons and mass surveillance and it develops a sense of having legislations or to update legislations with ethical considerations in order to define the morality along with legality of actions in terms of mass surveillance, data collection and processing.

This thesis aims to develop a sense of awareness among average internet users about mass surveillance (irrespective of their internet knowledge), its possible techniques and its scope by explaining in detail some portion of Snowden's leaked documents and concluding it by having ethical analysis of mass surveillance in the light of Utilitarian thinking. That is why this document stresses more on theoretical aspects than on technical aspects while having easy to understand language so that any average internet user could understand the concept of Panopticons and mass surveillance from various dimensions.

The thesis begins with the explanation of internet layers and the possible activities that could be performed within those layers in first chapter. Second chapter moves towards the historical background and origin of the terminology i.e. “Panopticon” and explains the evolution of this conceptual terminology. Then it leads to the origin and whistle blowing by presenting an overview of contemporary Panopticism followed by defining some mass surveillance operations.

Third chapter explains different aspects of surveillance in relation with reasons, privacy, and anonymity by elaborating cause and effect relationship among these three aspects. The next topic then explains the scope of mass surveillance unveiling multiple levels which could be a part of mass surveillance in terms of data collection by the surveilling authorities.

Fourth chapter focusses on what kind of actors could possibly be involved in surveilling activities in any society. And through which ways their surveilling tendencies are fulfilled? This chapter uses Snowden’s revelations as a case study. Moreover, it highlights the actors involved in mass surveillance both on private and government scale along with their most common methods in practice.

Fifth chapter presents the ethical analysis of Snowden’s Act of revelations, top three accusations posed on Snowden by US house of representatives and mass surveillance by state and non-state actors by considering Utilitarianism as a base ethical theory. It begins with the reasoning behind the choice of Utilitarianism and then it proceeds with ethical analysis.

Sixth and the final chapter addresses legal and cultural implications in relation with ethics.

1.1 Research Methodology

Pragmatically, this thesis is based upon Qualitative research approach which further chooses a mixture of methods in order to collect and analyze the literature, data and to become more descriptive/interpretive in presenting the arguments, contradictions of situations and deduced outcomes, so that multiple perspectives of the topic could be explored. Primary focus of the thesis is to analyze the scope, actors and techniques that are involved in mass surveillance with a motive of viewing all these three factors from ethical point of view. The reason behind choosing Qualitative research methodology is that it allows people to deduce inferences based on their experiences while using their humanistic instincts. It is primarily concerned about the human understanding of certain issues in an interpretive way [4]. Because world around us cannot be considered as something independent of human perceptions/interpretations, which are consequently created by the interaction between individuals and the world around them [5]. That is why this approach is best suited for the chosen topic because the topic is more inclined towards humans involved in the activity than the technicalities. Moreover, Qualitative approach has been referred as an Umbrella, which contains many sub-types of research methodologies under its wider framework [6].

In the light of the chosen topic, the amalgam of two sub-techniques of Qualitative methodology has been adopted i.e. Process Tracing and Case Study. The research being a mixture of both these approaches facilitates to deduce inferences along with highlighting cause and effect as well at some points where needed. Because primary motive of this thesis is to unveil some facts by connecting the dots and to develop an understanding of the core topic through them, that's why instead of relying solely on any particular research methodology, mixture of two methods has been adopted to achieve the desired flexibility in this research methodology. This type of research methodology of using tools from the same research paradigm (Qualitative or Quantitative) is known as mixed-method approach. Mixed-method research is often denoted as methods-centric approach as well. In case of methods-centric approach, methodology is usually isolated from rest of the research model and it appears at the last in design sequence [5].

Process Tracing is being considered as a fundamental tool of Qualitative research approach. This approach is primarily based on drawing casual inferences by deducing theory that is extracted from the descriptive literature [7]. It is a combination of many steps that represents a series of events (which are supposed to be chronologically considered and analyzed) to explain a certain occurrence with the motive of explaining cause and effect.

On the other hand, case study also comes under the wider-framework of Qualitative research paradigm which can be defined as a detailed investigation of a certain happening within its natural setting, in order to draw conclusions out of it in relation to our hypothesis [8]. The primary difference between Process-tracing and Case-study methodologies is that former one gathers the data chronologically in order to justify the cause and effect for drawing casual inferences while the latter one focusses on one particular happening for an in-depth analysis in order to explain every minor and major detail linked with our hypothesis.

The thesis begins with the exploration of relevant literature which initiates with digging the layers of internet and then tracing the flashback of Panopticons and its current shape which has been rapidly changing since last few decades, in spite of the fact that Panoptic mentality is much more older which leads back to eighteenth century. The next step proceeds with bridging the ancient conceptual Panopticon with the current day mass surveillance and highlights the factors which reflects its exact replica consequently implying that how contemporary surveillance fits perfectly in the definition of Eighteenth Century's Panopticon.

Process tracing's implications starts from the indication of events that compelled the authorities across the globe in different parts of the world to fabricate the mass surveillance programs, however the inception of this concept led the situation entirely in a different direction. For case-study, one of the biggest breaches of documents in intelligence community by a former contractor has been taken into consideration for the purpose of highlighting different methodologies and the actors involved in them through which mass surveillance have been on-going since more than a decade. Moreover, this thesis also focuses on various dimensions that are directly or indirectly linked with mass surveillance, which includes privacy, anonymity, reasons behind surveillance, laws, culture etc. The flow chart of the research design is shown in figure 0.

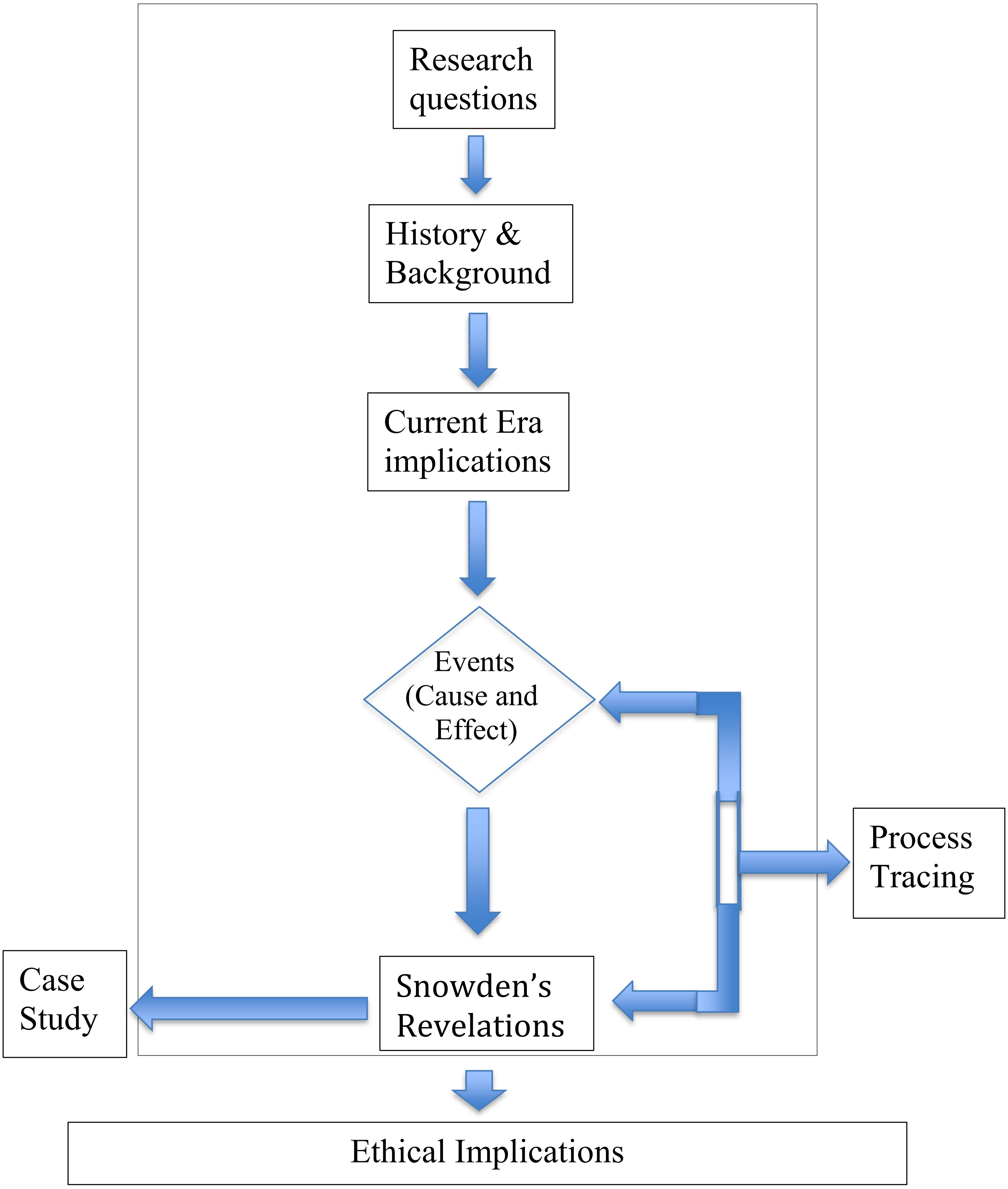


Figure 0: Research Methodology

Both the research approaches that are being used in this thesis are intertwined due to which it's not possible to isolate both of these processes in the research design or to draw a border line between the steps on which either of the approach is applied. Research questions raised in this document are as follows,

Q1: How the ancient conceptual Panopticon replicates the current era's mass surveillance?

Q2: What are the factors that must be fulfilled to call any actor as a Panopticon?

Q3: How utilitarianism distinguishes between ethical and unethical mass surveillance?

Q4: Who are the most prominent categories of actors that are involved in contemporary Panopticism and how they are doing it?

1.2 Digital Era

As per the scope of this thesis, the term "Digital Era" implies the age of internet or the tenure that began with the inception of internet. Internet has acquired almost every walk of human life, whether it's a day to day routine life activity, the study of blackholes, medical research, entertainment, journalism, international trade, international relations, education system, warfare or even political infrastructure, use of internet has become a primary as well as mandatory need and want. This prevalent use of internet has brought humanity in the era where every kind of information is just a Google search away, where every connection with anyone from any part of the world is just a click away irrespective of distance. Activities related to internet are not just confined within the networks as something abstract instead internet based activities and access has become a part of our tangible world as well e.g. home systems can be connected with internet including our doors, security cameras, air conditioning, door locks, laundry machines and even showers. This situation of connecting routine life tools with internet is also known as "Internet of Things".

Similarly, internet has also brought us into an era of data explosion where in every single second, data of millions of tera bytes is being generated worldwide. Where communication systems are even faster than the speed of sound, where even rebellions have been started through social media on internet in which Arab Spring is the most well-known one [3]. Hence proved, that internet has become one of the basic elements of human life and it can be enormously useful almost in every possible dimension of our life.

The question about whether the activities happening through internet are ethical or not contains many elements in it, in which some of the most common elements are Privacy and security of information. Why only information? Because over the internet, information is the most precious asset anyone can ever have. Information can further be categorized into sub-types e.g. documents, bank credentials, social credentials, passwords, email addresses, conversations, pictures, videos and every such piece of data which can be misused by anyone in anyway compels its respective owner to take some measures for its protection.

1.2.1 Layers of Internet

Having the knowledge of layers of internet is as important as having a driving license before driving. We can drive even without having a license but we cannot make sure of developing the road sense which can really be helpful for us to drive more safely and to prevent accidents, similarly, we can use internet without even knowing the layers of internet but in this way, we won't be able to familiarize ourselves with the vulnerabilities as well as the blessings of internet in a true sense. This section aims to develop an understanding of different layers of internet from the point of view of highlighting different activities that are being performed over there and the access of those respective layers to the public.

Internet is available in three different layers which are categorized based on many different attributes in terms of their usage, accessibility, the type of data it contains and the type of activities that can be or are being done over that particular level or layer. Those three layers of internet are i.e. Surface Web, Deep Web and Dark Web. Figure 1 has shown all the three layers along with the type of content available on each level respectively [9].

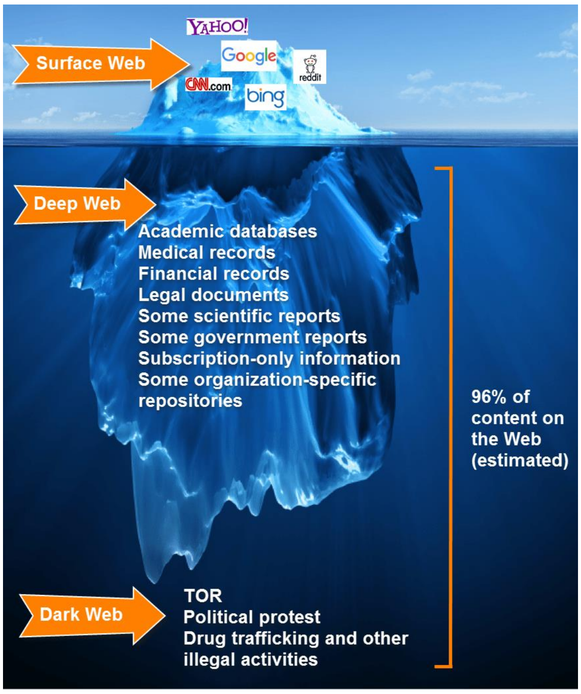


Figure 1: Layers of Internet

An average internet user belongs to the surface level of the internet in which he/she can access various social media sites, shopping sites, banking sites, news and journalism sites, games, freely available documents (books, journals, magazines etc.), media, entertainment sites, free porn sites and many freely available software's and applications as well and the list might be endless but within certain boundaries because Surface Web contains merely 4% of the total content that is available on the internet so, by this, we can easily assume that how enormous the other two layers are.

At second layer, there comes, Deep Web which contains mostly classified information. Classified implies the kind of information e.g. database of educational institutions, financial records, legal documents, copyrights protected text (articles, conferences, researches etc.) so such websites sometimes may or may not necessarily appears in search engines. The structure of Deep Web is bit more complex than a regular surface web. Because the content of Deep Web isn't indexed in regular search engines like Google, Wikipedia, Yahoo, Bing etc. instead, there are some special purpose search engines which are specifically required to access the content of Deep Web e.g. DuckDuckGo, Yippy, Torlinks etc. It is because, the kind of websites available on Deep Web usually falls in one of the following categories [10, p. 5],

1- Dynamic Webpages.
2- Blocked sites (the sites which requires us to enter CAPTCHA to access the content).
3- Unlinked sites or Orphan URLs (Uniform Resource Locator).
4- Private sites (websites that requires login credentials)
5- Non-HTML/-scripted/-contextual content
6- Limited access networks

The last and the deepest layer of internet is known as Dark Web, its name is self-explanatory so yes, it is primarily being used by terrorists, intelligence agencies, protestors, hackers, drug traffickers and almost every single human being on earth who is busy in doing something legal or illegal but necessarily being anonymous. It is also known by the name of Dark Net. This layer is basically the subset of Deep Web. This layer of internet is completely anonymous and it never ever appears in any search engine nor it can be accessed through a normal internet browser instead a special browser by the name of TOR (The Onion Router) is available for this purpose particularly. Dark web is not necessarily being used for illegal or criminal activities solely instead it is being used by governments as well for tracking criminals and for research purposes as well as shown in Figure 1 because almost 96% of the information is currently estimated to be available on Deep and Dark web so just like Surface Web, the usage of Deep Web and Dark Web also varies from person to person or organization to organization but yes one thing is for sure that unlike other two upper layers of internet, majority of the illegal activities are being done in the Dark Web. Why? Because whether we say it as the worst or the best part, but Dark Web provides the users with maximum possible anonymity while doing any good or bad activity over the internet, that's why majority of the crimes are being executed in Dark web. Dark Web was initially created to harness secure communications by escaping censorship as a way to guarantee free speech but the evolution of Dark Web in terms of activities going on over the years has really made this layer quite a shady and controversial platform [10, p. 5].

Along with containing major part of knowledge across the internet, Dark Web has given rise to numerous heinous activities leading from child pornography and drugs to hiring a contract killer and may be having fake documents of any region across the globe being extremely anonymous which has consequently made Dark Web as a safe haven for any kind of criminal activity. Due to all such factors, dark web has become quite a perplexed platform to be explored, monitored or controlled because along with anonymity, it brings extreme vulnerabilities to human psychology and mindset as well by giving rise to numerous possibilities of executing criminal activities anonymously which consequently affects the behaviour and human activities both virtually as well as tangibly.

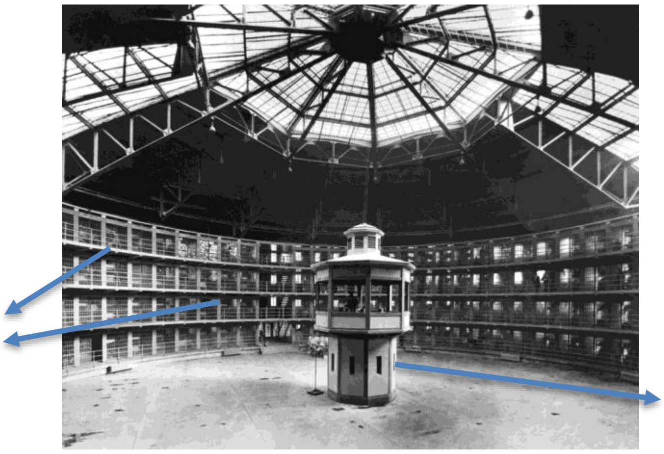
So, in this regard a famous American Businessman says,

The ***Internet*** *is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.* -Eric Schmidt[1].

[1] Eric Emerson Schmidt is an American Software Engineer and Businessman who currently chairs America's Defense Innovation Advisory Board.
https://www.forbes.com/profile/eric-schmidt/#7bf5a102138e

Chapter 2: Panopticons

Cambridge dictionary explains this word "Panopticon" as "A Prison with cells (rooms/lockups) in a circle so that the prisoners in them could be seen at all times from the tower made in the center of that circular prison" [11]. So, according to this definition, there is a tower with guards in the center of a circular prison who can keep an eye on all the prisoners in all the lockups whenever they want without letting the prisoners know that when they are being watched and when they are not as shown in Figure 2 having the blueprint of a panopticon prison [11]. This is a literal definition of panopticon. But this term is quite popular on internet since last decade especially since the inception of social media's popularity over the internet. The reason behind the popularity of this term over the internet is because of a very strong resemblance between panopticon and current social media, other web-companies and even governments which will be discussed in later sections of this thesis.



Prisoner's cells in circle [11].

Central Tower having guards for keeping eyes on prisoners [11].

Figure 2: Panopticon Prison

2.1 History & Background

The famous Panopticon building as described above was designed by Jeremy Bentham (1748-1832) in Eighteenth Century. Bentham is among one of the founding fathers of ethical theory of modern Utilitarianism, a political reformer, and a jurist as well. Although the core tendencies behind the motivation of this theory were observed much earlier, but Bentham was the first one to formally present this theory [12], [96]. Utilitarianism is an ethical theory which establishes the morality of any action based on its consequences.

Bentham states that this kind of "All-seeing" confinement-based punishment is more humanistic than regular torture techniques. And above all, this design of prison allows to maintain a thorough surveillance by using minimum possible resources and without the knowledge of the prisoners and this is exactly what synchronizes with the theory of Bentham about defining any action's morality by viewing the consequences produced/achieved out of it. The story did not end here instead Bentham wanted to take it to next level by making this prison as a profit-making organization through its privatization in which he himself wanted to become the first contractor for this project.

And this is what led to the rejection of his idea. The design and implementation part were widely viewed and accepted at that time but the notion of opening the Panopticon for private contractors is what led to the complete rejection of his idea. Because Bentham viewed the prison as a private enterprise for making money through the labor of prisoners. This one specific financial element completely turned down his idea because the authority and control of the prison was believed to be best kept under government authorities and bureaucracy, consequently implying that prison labor should not be capitalized [13].

The design of Panopticon represents a unique mentality which kept on evolving over the years and we still have it in the most refined form ever. Let us have a look at the design of the Panopticon building and have a look at the mentality behind it. Because the physics behind the design of the prison was more inclined towards handling the human psychology without forcing them to do anything specific which consequently prevents compelling them forcefully to drive their psychology according to the needs of the designer of the building or the guards or supervisor of the prison. So, according to the design of Panopticon, the prison guard should be placed in the center of circular prison in a tower. And prisoners must be placed individually in each cell being isolated from each other. The prison cells should be made as much visible as possible while the guards in the tower must be made as much invisible as possible by using high beam lights and screens to hide the guards from prisoners completely. Prisoners must never know when exactly they are being watched but they must have the conscious and constant realization of being watched all the time and this is the core principle of a Panopticon. And that's exactly why, prisoners would surely behave all the time with the fear of being watched because of being unable to recognize the pattern of this mode of surveillance. So, now every single prisoner must be watching him/herself consequently bound to respond to the panoptic mentality of this prison. And this is what makes the guards dispensable because the prisoners can never find out if the guards are even present in the tower or not, if we are being watched or not and when we are being watched and when we are not, consequently leaving the prisoners completely clueless about this surveillance and this mode helps to improve the behavior of prisoners as well as to maintain peace in prison [13]. So, in this way, by using modern terminology, we can tag this situation as of "Automating the Surveillance" in the Panopticon prison.

Bentham was primarily concerned about having the panoptic structure in terms of prisons solely, but this kind of utilitarian design can be implemented anywhere i.e. schools, army barracks, hospitals, factories etc. because of having obvious advantages not necessarily for keeping an eye on workers/prisoners/patients/soldiers with the intention of punishing them but for keeping them safe as well. So, now we can conclude the entire philosophy and mentality of a Panopticon in five points as follows [13],

1- The observer must not be visible from the position he/she observes.
2- The object under observation must have the realization of being visible and being surveilled.
3- Surveillance is made simple and straight forward which shows that most functions of surveillance can possibly be made automated.

4- Surveillance is being made depersonalized because the observer is not important and this anonymous nature of this kind of surveillance makes possible for anyone to observe who is involved in this operation/function.
5- Panoptic surveillance can be used to research human behavior as it facilitates the systematic collection of data about human lifestyle.

This idea of Bentham just merely presented the prototype of a mentality regarding the establishment of mass surveillance but even now-a-days, the organizational infrastructure around us presents this same mentality consequently giving us an overall impression of surviving in a panoptic society. What was the intention of Bentham behind presenting this idea and whether his idea failed or succeeded in his time respectively is entirely a different argument? But his idea not just merely represents a prison or a building instead his idea can be seen everywhere in current society which will be discussed in later parts of this thesis. The society we are currently living in presents an exact replica of a panoptic prison irrespective of the nature of organizations, lifestyle, financial status, cultural or religious values, gender, and age group etc. Hence, Bentham's idea of a panoptic prison represents a mentality which can be applied anywhere to maintain a control over masses without forcing them to do anything.

In terms of Panopticism, there is one French philosopher Micheal Foucault (1926-1984) whose criticism and views on the idea of Panopticon mindset also holds significant position in historical perspective. Foucault is the first one who used/introduced the term Panopticism which he derived from the theory of Bentham's panopticon and that term then gained the popularity for defining the Bentham's Utilitarian theory in general. Panopticism is a theoretical formulation of surveillance society based on the Bentham's project of panoptic prison having an all-seeing guard/inspector [14]. Foucault rejected the idea of having a panopticon prison as a humanistic approach instead he stated that it is not at all humanistic because it is just another way to exercise power. Foucault describes Panopticism in his famous book *Surveiller et punir* as [15, p. 210],

"*Le panoptisme, c'est le principe général d'une nouvelle a anatomie politique » dont l'objet et la fin ne sont pas le rapport de souveraineté mais les relations de discipline.*"

It translates as, Panopticism is a new political anatomy in which sovereignty has been replaced by discipline.

Although Foucault called it a political anatomy, yet it is a social anatomy as well in the light of current era. Foucault further states that panoptic mindset focusses on replacing sovereignty with more subtle and hidden authority. So, this new kind of authority exercises its power by objectifying its desired subjects by creating more and more knowledge about them. Basically, this Panopticon mindset based on disciplinary power comprises of constant drills, reporting, regulations, testing, setting up limits and not just mere surveillance. Through all these methods, surveillance is being primarily used as a prominent and visible bait which makes sure the maximum possible control over any individual/subject. Hence this disciplinary mechanism exercises its power by maintaining a frequent gaze through its all-seeing eye. [13, p. 112]

2.2 Panopticism in Digital Era

The concept of Panopticism derived by Michael Foucault from the Panopticon structure presented by Jeremy Bentham holds a pivotal position in explaining the current day mass surveillance. Moreover, it emphasizes on the fact that gradually but definitely, we have become the part of a panoptic society irrespective of cultures, regions, or organizations. The globe has not just been converted into a global village instead more precisely we can say that it has become a Panopticism oriented global village. This is the reason due to which Bentham believes that panoptic structure is needed to encourage the subjects to move towards self-discipline, consequently preventing them from misbehaving within the premises, while Foucault contradicts from this mentality of Bentham in his book Discipline and Punish (1975) and states that panoptic mindset has been actually presented to subjugate the citizens in any society. Foucault looked at this panoptic structure and mentality in terms of using power and its increased bureaucratization in modern world [16].

In current era which is known as digital era or internet era as well, the word “Panopticon” implies a metaphorical framework to represent the mass surveillance going on via using various methods. In current era, the panoptic surveillance has been deeply rooted in almost every single aspect of our society including organizations (both government and private), public places, hospitals, educational institutions and so on. If we compare modern day Panopticism with Bentham’s structure, then apparently, we do not find any resemblance because we do not get to see a visible tower in the center in any aspect of our life around us. So, in this way we do not even know that from where anyone can possibly watch us? This gives rise to a very important question which needs to be addressed i.e. The fact that we do not know that we are being watched indicates that may be, we are being normalized in a way the Panopticon was intended to correct the behavior [16]? Because in the Panopticon prison, the prisoners were under a constant fear of being watched and the ignition of that fear among prisoners was the core idea behind the design of a panoptic prison which was supposed to become a new normal for the prisoners. But in modern day surveillance, there are not any visible proofs, central towers or markers which could give us the sense of being watched for fixing our behavior. This is what has exactly happened with us that we have become so normalized with this surveillance that we do not even feel anyone spying on us anymore, and that’s how modern day Panopticism has established. This is just one dimension of modern day Panopticism, that is why the story does not just end here as there are much more hidden details which must be considered in this regard before drawing any conclusions.

Contemporary Panopticism has been penetrated in our society via various actors behind it both through government as well as private sources. In terms of exposing mass surveillance both by state and non-state actors, Edward Snowden[2] is being considered as

[2] Edward Snowden is a former contractor of American Intelligence Agency named NSA (National Security Agency) and he leaked highly classified documents of American intelligence community regarding mass surveillance activities of American Government in 2013. Since then, he is residing in Russia on Asylum. https://edwardsnowden.com/

among the top whistleblowers who safely yet drastically raised awareness among people. In terms of mass surveillance by organizations especially search engines and social media owners, numerous sets of events took place which made their way in raising public awareness consequently exposing the mass surveillance techniques established by social media giants and search engines. In current era, Panopticism is primarily associated with the social media or with search engines although governments are also involved in executing their own mass surveillance through various techniques but people are more concerned about the social media, because majority of us are subscribers of various social media platforms, so that is why while using the word Panopticon now a days immediately diverts our attention towards social media e.g. Facebook, Twitter, Instagram etc. and their owners Mark Zuckerberg, Jack Dorsey etc. To a certain extent, that is authentic, but there are many other actors as well that fulfills the criteria of being a panopticon in which governments as well as many other private organizations involved other than social media. Now the question is that why they (social media/governments/third parties) are being called as Panopticons when they do not even work as a watchmen or guard in a prison having circular architecture as shown above in Figure 2? Neither they own such a prison in which prisoners are being locked and monitored. The answer to this question could be the criteria which makes all of them as Panopticons and that criteria is the mode of their surveillance over the activities of their subscribers and the general public they have on their respective social media sites and on various platforms across the internet. Every single activity of every single subscriber as well as internet user is being monitored without the knowledge of users and whoever is monitoring every user is completely invisible, so this is what brings these social media owners, governments and other private organizations closer to be called as Panopticons. One piece of the puzzle was still missing since before Snowden's revelations, that is why till his revelations all such social media giants, governments and other companies could not get tagged exactly as a Panopticon presented by Bentham. And that piece of the puzzle will be addressed in the last of this chapter.

Since last decade, social media sites have become primary source of maintaining a very precise and in-depth surveillance over masses. The free subscription to any social media site is not free at all anymore not from monetary point of view but in terms of privacy protection of our every single piece of information that we share over there. In this way, we are living in the era having a vast grid of surveillance which makes our personalities completely visible all the time even if we are offline. Social media has basically shaped our behavior in such a way that we tend to share every or most of our daily activities there, about what we are reading, eating, drinking, watching, where we are travelling, whom is accompanying us and even what we are thinking in the form of status updates. In this way, anybody reading our status becomes aware with our activities and even with our location as well. In case of location updates, sometimes, some automated options work out themselves. So that is how our behaviors are being controlled and modified by modern day Panopticons primarily through social media without imposing any torture methods or force. And this is what clearly endorses the concept presented by Jeremy Bentham and justifies the arguments of Michael Foucault as well.

In modern day Panopticism, we are also partially responsible as we have also agreed to share our information freely and publicly consequently giving a free pass of mass surveillance to these Panopticons. Current day Panopticism is much more subtle and insidious than the one presented by Bentham because nowadays, Panopticism isn't merely confined within prisons or prisoners instead the entire society has been converted into a panoptic structure without using any force but by using manipulative methods which are constantly playing with minds of people and altering their behavior in a way these modern day Panopticons intends to achieve. The watch tower has been replaced with AI (Artificial Intelligence) algorithms, security cameras etc. for collecting data and making profiles about the activities of people which later involves data trafficking and its capitalization and the list goes on [16]. Hence proved that in contemporary Panopticism, most of the social media sites primarily represents an exact replica of what was previously known only as a circular prison. Moreover, it also justifies the argument presented by Foucault of declaring Panopticon as a mechanism of exercising power in a different way.

2.2.1 Origin, Background and Whistleblowing

Contemporary Panopticism holds a significant position for many governments as well as for various domain owners due to multiple reasons. Current mass surveillance can be blamed upon various reasons in which war on terror could be one of the many primary reasons but the origin of this Panoptic mentality leads back to few specific incidents which are important to be considered in order to understand that what caused this Panoptic mentality to be developed among technology elites and governments. Although the Subway Sarin attack (March 20, 1995) Tokyo, Japan proved to be quite a disastrous one which took the life of 11 people and injured hundreds [17], yet there are not enough evidences which could declare Tokyo Subway Sarin Attacks as the starting point for the inception of mass surveillance activities but yes it could be considered as one of the many reasons. Similarly, from 1995 to onwards, right after six years, the attack on World Trade Centre on 11th September 2001 [18] aggravated the situation more which consequently and gradually but definitely tended the governments and security agencies across the globe to plan some pre-emptive measures in order to predict the possible threats in advance for the purpose of eliminating them as well as preventing any catastrophic attack in future. So that's how series of different events across the globe shaped various surveillance tendencies in the name of precautionary measures. But despite this fact, we cannot pinpoint any certain event which specifically caused the inception of mass surveillance illegally or legally, publicly, or privately, authorized, or unauthorized, informed, or uninformed and ethical or unethical.

Mass surveillance used to be quite a confined activity in the early days of internet which was specifically restricted or popular within closed walls e.g. hospital wards, prisons, schools, offices etc. and the primary methodology for surveilling such sites used to be CCTV (Close Circuit Television) cameras and there was no opposition in maintaining such sort of surveillance techniques as it was a clearly visible source of surveilling masses under certain conditions at certain times and in certain locations. But things changed at that very moment when masses got to know about something much more enormous than that and this is what actually happened through some whistle blowers in which Edward Snowden is still being considered as the most significant one as he proved to be quite an eye opener across the globe.

Till the end of last decade, contemporary Panopticism was justifying every single condition of the actual panoptic prison presented by Bentham except one thing that masses had no idea that even if they are being watched or not and to what extent, while in case of Bentham's Panoptic prison, every single prisoner was supposed to have the fear and conscious realization of being watched all the time. Masses were quite freely roaming across the internet without having the fear of being watched because of being unaware of the facts and intentions of the giant organizations and governments around the globe. This carefree roaming over internet kept going on by masses until in 2013 Edward Snowden burst everyone's bubble of this carefree surfing by exposing major organizations and governments involved in secret mass surveillance activities after which he had to flee to Russia for asylum or else he might have been executed or jailed by now in USA. Some of the mass surveillance programs he shouted out about are as follows [19, pp. 3-7],

- PRISM.
- Upstream.
- XKeyscore.
- BULLRUN.
- MUSCULAR.
- FAIRVIEW.

By looking at the primary motives of all these programs introduced below will surely give us a glimpse of a bigger picture about how far things had gone in terms of mass surveillance that were exposed by Edward Snowden.

2.2.1.1 PRISM

This program was designed to access information from USA's biggest technology companies which includes Apple, Google, Microsoft, Facebook, Paltalk, Yahoo and AOL [19, p. 4].

2.2.1.2 Upstream

This program was designed to intercept the international internet traffic and to switch it between two specific carriers by tapping the underwater fiber optic cables without any warrant [19, p. 5].

2.2.1.3 XKeyscore

This program included the largest data collection of every single possible internet user including everything he/she does. The data included phone numbers, email addresses, IP addresses, port numbers, cookies, geolocations etc. [19, p. 5].

2.2.1.4 Bullrun

Under this project, NSA aimed to inject planned backdoors and vulnerabilities in encryption systems, telecommunication technologies, operating systems and in many other routine life technologies that were under the use of public [20].

2.2.1.5 MUSCULAR

In this program, NSA (National Security Agency)[3] managed to infiltrate the private fiber optic cable of Google's own network and the links between the Yahoo's and Google's data centers [21].

2.2.1.6 FAIRVIEW

FAIRVIEW program aimed to gain access to international cables, switches and routers through internet service providers and various telecommunication companies [21].

NSA didn't even stop or finally started relying on these above mentioned programs instead the list of NSA activities in order to access every nook and cranny of internet by becoming an all-seeing eye on internet never actually stopped and they kept on developing different programs in order to tackle the ever changing scenarios on internet. Hence, the list consisting of mass surveillance done by NSA kept on getting longer and longer and the above-mentioned programs are merely few examples out of that long list. Moreover, NSA worked with four other governments including Australia, Canada, New Zealand, and UK and called this alliance as "Five Eyes". But this alliance is not just confined within these five governments, instead they executed their activities across the globe in collaboration with many other governments as well [22].

Snowden's revelations unveiled three primary actors responsible for mass surveillance which are as follows,

1- Governments that are engaged in mass surveillance, e.g. USA along with its four other partner governments as mentioned above.
2- Organizations sharing their data with the governments for mutual benefits or trade or being under pressure [22].
3- General public sharing their activities through online interactions primarily through social media or cell phones [22].

From this above discussion regarding the background and whistleblowing in terms of mass surveillance, we can clearly conclude that in current era, Panopticons are of two types, i.e. governments and private organizations. Both works independently as well as in coalition with each other. Hence, the Snowden's revelations did not just expose the NSA's activities of mass surveillance instead it unveiled mass surveillance activities going on globally both by government as well as by private organizations. And this awareness is what makes the overall atmosphere more Panoptic as now we are aware of it and this is exactly what Bentham presented in his design of his Panopticon that prisoners must be aware about being monitored all the time consequently having a fear of correcting their behavior. Hence, Snowden's revelations added the missing piece in the puzzle of current day Panopticism and that was "awareness about being monitored". Although the contemporary Panopticons didn't want to add the awareness part in their mass surveillance instead they wanted to keep on maintaining

[3] NSA is a national level security agency of the USA's department of Defense and it works under the command of Director of National Intelligence. Its core functionalities include global monitoring, data collection and processing both for foreign and domestic intelligence purposes. https://www.nsa.gov/

their precise mass surveillance without letting anyone know about it and this is what was happening since before the revelations of Snowden.

Chapter 3: Surveillance: Cause & Effect

Surveillance being an ancient tendency can be defined in many ways especially english vocabulary provides us with wide range of expressions in this regard e.g. control, supervise, gaze, stalk, track, spy, follow, eavesdrop and the list goes on. Highlighting the origin of this term leads to a French word *Surveillir* which was further originated from a Latin word *Vigilare,* which implies that something insidiously criminal or threatening is going on behind closed doors. Hence this ancient definition implies something related to security agencies or police in general because security providing organizations are supposed to take care of any sort of criminal activitiy going on. But in case of contemporary society, surveillance holds a much wider perspective. There are many verbs that can fit within this term but many ethical theorists and philosophers emphasizes on one particular verb in this regard which is "To Control" consequently presenting a very narrow definition [72].

Hence, this chapter contains the "Cause & Effect" oriented discussion pertaining to surveillance tendencies. It discusses the possible causes behind a surveillance tendency and how such tendencies consequently influence different aspects of human life especially Privacy and how it invokes the concept of Anonymity. Morover, it illuminates the scope of Mass Surveillance as well which is primarily based on four different strategical plannings depending upon the needs of a surveilling authority. Associating surveillance merely with control narrows down its scope consequently shoving down a rigid concept which confines our thought process. That's why this chapter focusses on others factors as well in parallel to control i.e. protection, security, safety, training, brought up, conflict management etc. which declares surveillance tendencies more of a situation oriented need.

3.1 Reasons

Understanding the mentality or reason behind surveillance leads towards a better understanding of the types of surveillance, its scope, purpose, and impact.

Surveillance is a very generalized terminology which can be defined in many ways as discussed above and it comes in different sizes and shapes with varying impacts which can either be positive or negative. Surveillance is not merely a mentality but for some reasons to some extent in some particular conditions, it can be fairly viewed as a justified and rational need as well e.g. in case of prisons for monitoring the criminals consequently trying to maintain peace and to refrain from any kind of inconvenient and drastic happening because prisoners are in prison for a justified reason after being accused, caught and declared guilty for the crimes they committed. This kind of surveillance could be considered as a mean for not just to develop control but to prevent any kind of unwanted activity from the criminals especially the brawls amongst them which is always the most expected activity that can happen in prisons. Hence, it implies the conflict management, security as well as training of prisoners consequently negating the fact that control is the only thing surveillance could be aimed for.

Similarly, surveillance can be done over kids in order to monitor their behavior and to prevent them from doing anything wrong, unsafe or unethical consequently shaping their personality and encouraging them up towards an ethical and safe brought up for making them a better person in future. This type of surveillance needs to be done for the sake of both management as well as influencing the kids by teaching them values and then monitoring their behavior accordingly. Another example of surveillance could be monitoring the employees or labor at the workplace to prevent any kind of workplace hazards and to prevent the entrance of any unauthorized personnel. Similarly, surveillance could also be done in workplaces for the sake of reward and recognition of employees. Hence, it also represents reasons behind surveillance which are other than "To Control".

David Lyon[4] holds a significant position in the field of surveillance studies, so according to him, surveillance is a vast yet critical concept which can be viewed as any systematic and routine activity by having focused attention on personal details of any entity for the purpose of influence, control, management and entitlement [23]. Hence, the examples based on situations described above syncs perfectly with the set of reasons behind surveillance presented by David Lyon i.e. influence, control, management, and entitlement.

From this above discussion we can conclude that surveillance should not always be seen as something negative, instead in many cases, it can be proved useful as well, so instead of tagging "Surveillance" as a terrified, heinous or enforced activity, we need to focus on the reasons behind it because it's the reason behind surveillance which makes it ethical or unethical.

3.2 Privacy

The term "Privacy" cannot be defined by a generalized definition when it comes to consider it in connection with surveillance because privacy can vary from context to context, situation to situation, location to location and similarly many other aspects can be considered under the umbrella of privacy e.g. privacy could be entirely a different entity for a vlogger or any social media influencer, similarly it could vary for a movie actor/actress or an athlete in some other dimension and when we consider a regular social media user, privacy might have a different meaning for him/her, when we talk about a cybersecurity expert, he/she might have entirely a different perspective in terms of his/her understanding and needs regarding privacy, so that's why it's hard to enclose the privacy in a box having hardcoded set of rules, yet there is a need to define boundaries or a framework which could cater the needs of everyone wandering over the internet in anyway.

Irrespective of the reasons or definitions given to privacy, one thing is ethically as well as universally hardcoded that privacy is a basic right of every human being because it provides an integral support to human dignity, self-respect and other essential values e.g. freedom of speech, freedom of choice, association etc. [24]. But the question is up to which extent privacy should be allowed? To answer this question, there are many factors which are needed to be considered, out of which impact, or in other

[4] David Lyon is a professor of sociology and he holds the charge of surveillance studies center along with heading as a Research Chair in Queen's University, Ontario, Canada. https://www.queensu.ca/sociology/people/faculty/david-lyon

words the pros and cons of that extent is necessary to be considered e.g. if a drug dealer is running a shady website over the internet and for an instance, we assume that he is completely anonymous so being a drug dealer, impacts of the privacy he owns will produce drastic and illegal outcomes with having debatable moral concerns. So, when we talk about defining the extent of surveillance, we also need to define the extent of privacy in parallel because both these entities go hand in hand, and they are inextricably connected.

Classic interpretations define privacy as a right to let alone the individuals [25]. So according to this definition we can consider privacy as someone's control over his/her own information which neither gets viewed by others nor the respective owner experiences any kind of external and unwanted disturbance and the owner is authorized to use his/her privacy/information anyway he/she wants. To underpin my own argument given in above paragraph about the extent of privacy, we need to have a look on the article 8 of ECHR (European Convention on Human Rights) which says,

"

1- *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2- *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."* [26, p. 7]

Hence, the European Convention of Human Rights clearly defines the extent of privacy plus it highlights two important factors in terms of privacy,

- Privacy not necessarily means the privacy of an individual from organizations or from governments instead privacy matters among individuals from each other as well.
- Secondly, it points out that privacy can be exercised in anyway except in ways which violates legal boundaries or become a threat against national integrity anyway or if it leads to any kind of criminal offense or it tarnishes moral values in anyway.

Hence, this article 8 of ECHR really defines very solid grounds for drawing a border line for individuals as well as for organizations/governments in terms of privacy.

3.3 Anonymity

Surveillance and anonymity also walk hand in hand just as the case of privacy. But privacy and anonymity are two entirely different entities, although they are being confused or conflated with each other especially while discussing information security related issues. But as a matter of fact, both are two entirely different dimensions. To define anonymity, a famous English proverb can really bolster our explanation about anonymity, which is as follows,

"Necessity is the mother of invention"

So, without the shadow of doubt we can blame the rapidly growing surveillance tendencies as a cause that gave rise to anonymity since last one and a half decade. Privacy is a state of having to protect one's own information/acts despite having traceable and identifiable information/acts, while anonymity inverts the situation by 180 degrees because anonymity is the state where someone becomes unidentifiable intentionally to the maximum possible extent. So, every anonymous individual has a privacy for sure but not every private individual is anonymous. Anonymity could be maintained in various ways, for example by covering face, through wigs, through plastic surgeries and so on and so forth. But in the case of internet, anonymity can be achieved by using entirely a different mechanism unlike real life scenarios e.g. by having fake ids followed by fake email addresses, by using TOR (The onion router) etc. TOR is the most popular and most effective way for becoming anonymous over the internet but still in some extremely rare cases, it can be tracked which as well is very highly unlikely and it requires highly specialized skill set. So far, many national or international jurisdictions does not address the issue of being anonymous [24]. So, that is why this anonymity is a home to both legal as well as illegal activities over the internet which consequently plays an important part in real life scenarios of individuals in parallel with their online activities. Deep Web and Dark Web are the best examples in this regard which can provide maximum possible anonymity to users for executing various activities across the internet (Refer to section 1.2.1).

3.4 Scope

Defining the scope of surveillance is like searching a needle in haystack because we are living in the era of data explosion where millions of tera bytes of data is being produced on daily basis across all the three layers of internet. Where every other day a new vulnerability and back door is being exposed meanwhile fixing the previous ones. Where masses are getting more and more aware about their privacy as well as anonymity consequently using more hidden platforms to stay private as well as anonymous.

To tackle the surveillance or more precisely mass surveillance in this complex era of data explosion, usually four different strategies can be observed to theorize the scope of mass surveillance somehow which are as follows [24],

1- Foreign vs National.
2- Downstream vs Upstream.
3- Targeted vs Bulk data collection.
4- Metadata vs targeted data collection.

These four ways represents four different mindsets based on requirements of any surveilling authority (Government or Private).

3.4.1 Foreign vs National

This comparison between taking a decision for drawing a borderline between national and foreign mass surveillance is based on quite a hypocritical mentality of governments because whatever is considered as legal by domestic agencies on foreign lands is considered as illegal on a national land by foreign agencies at the same time [24], [27, p.

37]. Masses are usually divided in two categories in this regard i.e. Nationals and foreigners. But nationals are further divided into two categories i.e. the born nationals and the migrated ones who later on gets the nationality and then comes tourists or visitors who are residing just for a particular span of time and then they go back once their purpose of stay is done or permission from immigration expires.

Distinguishing the foreign vs national mass surveillance is primarily based on two factors which are as follows,

1- Foreign mass surveillance is mostly a part of classical espionage techniques which are directly connected to military, political and many other national stakes.
2- While the domestic mass surveillance is directly linked to every single citizen currently residing within the domestic boundaries and this form of mass surveillance has proved to be much more significant (from government's point of view) because governments can easily track any individual within domestic boundaries in case of foreseeing any possible threat call and that's how the freedom of any or every individual can be monitored as well as restricted and in extreme cases suspected individuals might face prosecution under domestic laws. [24]

The foreign mass surveillance underpinning espionage techniques is usually pretty much restricted than national mass surveillance, although it has become an international practice, yet its legality is blurred and in case of being caught, individuals who are providing the services of espionage on foreign lands are executed in most cases or subject to never ending torture consequently suffering a painful and slow death [28], [29]. Hence, mass surveillance is not merely done via tapping internet cables or tracking phone calls etc. instead it's also being done by using highly trained personnel both on national as well as on international scale but the scope through this method is usually limited to a significant extent which is mostly restricted to few individuals or one individual at a time.

3.4.2 Downstream vs Upstream

In case of cyberspace, surveillance tendencies primarily begin with choosing a location for initiating mass surveillance which further depends upon whether it is a mass surveillance within national boundaries or somewhere across the borders. Generally there can be two possible starting points of executing mass surveillance i.e. tapping optical fiber cables manually or hacking/intercepting satellite communications and this is known as upstream while the other way is that government asks the ISPs (Internet Service Provider), telecommunication companies or other owners of various private Internet companies to provide data (after having a court order as a warrant) and this is how the downstream mass surveillance is being carried out.

From government's perspective and as per their approach as well as control over masses domestically, downstream surveillance is a piece of cake in case of any suspected threat within domestic boundaries, because just a signed permission/warrant by a judge is enough to demand any kind of communications from the ISPs or telecommunication companies or any other Internet company for further proceedings/investigations and this is what exactly happens in democratic governments. Despite being so easy at government's end, still there are defined set of rules available in legislations which states that under which circumstances the identities of individuals can be infringed by government officials without their permission [24].

Project Tempora can be considered as an example of upstream surveillance revealed by Snowden because it involved tapping the fiber optic cables of internet. Similarly, PRISM can be considered as an example of downstream surveillance. Because, under this program, NSA had direct access to the servers of some of the major internet companies such as Google, Paltalk, Skype, Facebook etc. [30]. Details pertaining to both Upstream and Downstream surveillance are discussed in the next chapter.

3.4.3 Targeted vs Bulk Data Collection in Mass Surveillance

Both these terminologies are self-explanatory as clear from their names, yet they contain many dimensions within themselves. The term "Bulk" is related to the collection of huge chunks of data without targeting any specific individual but even in some cases, if there is a targeted identity involved in it, still the data can be collected in bulk e.g. if an unknown target is in San Francisco, USA, then collecting the data of phone calls of all the habitants of San Francisco will be considered under the bulk collection of data although the suspect is an individual. Hence, therefore in case of bulk collection of data there is no certain threshold which must be satisfied in order to declare it a bulk collection instead any collection of data in huge chunks can be called as bulk with or without using any specific target.

Snowden's revelations did not just unveil the mass surveillance programs consequently spreading awareness among masses instead it effected almost every single organization across the globe which was involved in any kind of surveillance activities somehow. Primarily it affected American organizations, so after these revelations US president formed a committee for re-evaluating and defining many terminologies related to surveillance activities of intelligence community. So, in this regard, the committee formed by US president presented a definition derived from the briefings of the IC (Intelligence Community) and this definition then became the part of USA's Presidential Policy Directive (PPD-28). It says,

"If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted" [31, Section S.1, p. S-1].

Although PPD-28 presented a definition, yet it is not concrete enough to cater the hardcore attributes and functional values of bulk collection, so for the time being we can agree upon any collection of huge quantum of data with or without specifying a certain target can be considered under bulk collection.

In case of targeted data collection, there is always a specific individual under the radar due to which intelligence/surveillance organizations tend to collect more and more amount of data until target is being caught or the requirements of surveillance are being fulfilled. In such cases, even if the individual is known, still its data collection could be out of two possible ways, i.e. only the data pertaining to that targeted individual could be kept under the radar or a certain area could be targeted within the location where he/she resides e.g. if the target is any individual living in Manhattan Street, New York, USA then, is there a need to only keep tracking the records of that person or should the records of entire block or entire city needs to be collected? It varies according to the requirements of the surveilling authorities. But this phenomenon can be better explained by using two words i.e. "Select" and "Collect". So, mostly in case of Upstream data collection (Which can also be called as bulk collection), usually first data is Collected and then the target is being Selected, while in case of downstream data collection, it goes the other way around and it becomes Select then Collect format and that's how we can actually differentiate between bulk data collection and targeted data collection [24]. But despite these two cases, there could be a third case as well in which Selection can be done in parallel with Collection on the run time. And that is how the scope of mass surveillance according to the quantum of data collected could be defined.

3.4.4 Metadata vs Targeted data collection

There are generally two types of data that is possibly being collected through mass surveillance i.e. it could either be some targeted form of data (e.g. email tracking, phone calls tracking etc.) or metadata. Metadata is generally defined as data that provides more details about other data e.g. Metadata of telephone calls will contain all the possible details about those telephone calls including the phone numbers, location, time duration of phone calls, frequency of phone calls and so on and so forth. In short, metadata provides complete set of details about any form of data. While in other cases, there might be some specific forms of data that is being collected during surveillance, e.g. the text of emails, the pictures uploaded on Facebook, the articles written on WordPress etc. The choice of using either of the two methodologies depends upon the surveilling authority and their needs which are always requirement oriented. That is why, we cannot draw a borderline between situations which could necessitate the collection of either forms of data.

Hence, the outcome of this discussion presents us with the scope of any surveillance activity from four different dimensions which are as follows,

1- Who is being surveilled? Domestic individuals/masses or foreigners?
2- What kind of methodology needs to be used? A secret taping of underwater fiber optic cables of internet or court orders are required to be given to internet companies for accessing the data of targeted individuals?
3- In which quantity data will be collected? Do we need to follow "Select then Collect" or "Collect then Select" approach? Which approach best suits to our requirements?
4- Do we need to collect metadata or we need to collect any specific data type?

All these four concerns mentioned above could state the possible scope of any surveillance activity as per requirements of the surveilling authority.

Chapter 4: Types of Actors Involved in Mass Surveillance

Internet being an omnipresent source of connectivity has been bolstering human lives in multiple ways since the very day of its inception not merely by providing connectivity but by providing constantly evolving improved ways of performing various activities as well e.g. entertainment, knowledge sharing, freedom of expression, journalism, research etc. Along with being so enormous at the same time, it could be so vulnerable as well depending upon the way it is being handled because of having intentionally created or naturally present loopholes consequently endangering values of the social fabric globally.

Out of many significant provisions, Social media holds the place of one of the most refined creations over the internet which brought the connectivity towards frequently enhanced centralization consequently providing a single platform just a click way for performing various activities which were supposed to be done via using multiple platforms before. Social media generally appears to be quite an enchanting, active and easy to access source of connectivity, knowledge sharing, media, socializing etc. But in parallel it appears to be a very smooth mode of fulfilling various surveillance tendencies as well, by governments, private companies and even by individuals consequently breaching privacy of other individuals. Contemporary life style contains social media as a part of routine life matters not for everything but for majority of the activities especially the ones pertaining to human recreation and that's exactly why, having any individual around us not connected over any kind of social media platform could be a rare finding.

This chapter addresses how the concept of keeping privacy evolved over the years consequently enhancing its importance and how technology has influenced this asset along with human behaviors as well. Then it discusses Social Media and the possible motives of mass surveillance with or without being in touch with government. The case of Snowden's Revelations has been presented to highlight the mass surveillance activities at government level and the possible methodologies used, respectively. Then it discusses some of the private internet companies other than social media that could be involved in surveillance activities as well. As a whole, this chapter addresses the concerns raised in fourth research question according to which it defines the actors that are possibly involved in mass surveillance activities and how they are fulfilling their surveillance tendencies consequently achieving the desired level of mass surveillance. Furthermore, it explains how all such actors operates with or without being connected with each other. In this chapter, both the state and non-state actors have been clearly distinguished and explained along with the methods they use for surveillance, respectively.

4.1 Importance of Privacy

Just like a normal public gathering somewhere across the road, in a park or in any event complex, social media is also a public place, so that's why privacy over there matters in the same way as it matters at any other public place. "Privacy in Public" seems to be an oxymoron, but it's a very important concept in a well-functioning democratic society because it provides freedom of expression, freedom of thoughts, freedom of association consequently preventing the confinement of ideas, interactions and expressions and gives rise to a free market of expressions, interactions and ideas [32]. In an era before information technology, it was the hardest thing to capture the movements, thoughts and ideas of one person let alone millions which consequently given people much more privacy as well as freedom but access in general was limited because there wasn't any rapid source of delivering our ideas to masses other than newspaper which might be a good way to broadcast our ideas among masses yet it was not as efficient source as we have now in the form of internet where we don't have to have the approval from anyone to publicize our thoughts among masses. Similarly, at that time, monitoring any proceedings of any public gathering used to take quite a lot of manpower and even then, there used to be no proper methodologies for collecting and analyzing large amounts of data afterwards.

Traditional theories treated privacy as of only an intimate and personal realm [33]. But until the inception of information technology, the real threat to privacy was not perceived. That is why before the age of information technology, privacy in public was largely protected either by social conditions in general or by the limitations of technology which consequently made the public information almost completely obscure. So, in this way, such obscurity of privacy in public was not a planned activity but its obvious reason was technological limitations. Due to this limitation, the large scale surveillance was more like a fairy tale which wasn't possible at all, and that's how, the surveillance used to be quite a targeted activity confined merely up to certain individuals by engaging man power for this purpose. But after the rise of information technology and especially the social media, the concept of privacy, obscurity and surveillance has changed entirely, and it has become quite a perplexed aspect of our social setup. There comes another argument which contradicts with the notion of limitation of technology and it states that,

"Technology, however, is not a sufficient reason to account for this change. Instead, it is better to think of a process of causal over-determination, where a confluence of factors make surveillance often appear as the most appealing way to advance any number of institutional agendas. Some of these factors include changing governmental rationalities, the rise of managerialism, new risks (or perceived dangers), political expediency and public opinion". [34, p. 2]

Hence, according to this argument, technology is not the only entity that has compelled the organizations to establish surveillance mechanisms instead we need to pay attention towards the causes and factors other than technology as well that gave rise to this mindset of maintaining organized surveillance protocols. In this regard, Managerialism or Corporate Culture, Politics and Public opinion are some of the most significant reasons behind the nourishment of surveillance tendencies.

Emphasizing on importance of privacy in public doesn't necessarily mean that there should be a restriction on posting things online anywhere on social media or having the kind of privacy in which any individual is allowed to do anything in private irrespective of the legality or morality of that act. Instead privacy in public means that there should be a restriction as well as limitation about the extent of data collection, analysis and attribute profiling both by the private internet companies as well as by the governments. Because mass surveillance tendencies either by governments or by private organizations has not just affected the social media users, instead it has affected people from all walks of life e.g. PEN[5] America published a survey of almost 800 writers from different parts of the world, and they found out that,

"Writers living in liberal democratic countries have begun to engage in self-censorship at levels approaching those seen in non-democratic countries, indicating that mass surveillance has badly shaken writers' faith that democratic governments will respect their rights to privacy and freedom of expression, and that—because of pervasive surveillance—writers are concerned that expressing certain views even privately or researching certain topics may lead to negative consequences. More than 1 in 3 writers in Free countries (34%) said that they had avoided writing or speaking on a particular topic, or had seriously considered it, due to concerns about surveillance, compared to more than 1 in 4 U.S. writers (27%) surveyed by PEN" [35, p. 5].

Hence, it's not only the social media users, that are concerned about the invasion of their privacy in public, instead writers, journalists, historians and even researchers are also concerned about a breach in privacy through mass surveillance, so that's why in order to shape a free and balanced society having freedom of expression, association, thoughts, knowledge sharing, transparency, integrity and dignity irrespective of race, color, region or religion and political setup, privacy is important for people from every walk of life, that's why it must be respected in order to prevent the social fabric from being disturbed.

4.2 Behavioral Manipulations

It is not just the government or the private organizations who are involved in surveillance, instead the readily accessible technological advancements have turned every single individual into a spy. Every single one of us is surveilling on someone to some extent e.g. checking the Facebook/Instagram of the Ex and seeing him/her enjoying with a new partner, meeting someone at the bar and then checking their social media profiles in order to know more about them, or in first few weeks of a relationship, reading some photos or posts having hidden meanings in case of not getting a reply back from the partner etc. And there are many such examples which have made this spying tendency as a normal behavior and this is what used to be known as stalking back in 90s. Just imagine up to which lengths one would've to go to spy on his/her Ex back in 80s or early 90s or earlier than that: May be breaking into his/her house, chasing him/her on road, workplace etc. so in short, it used to be quite a fatigued and hectic activity if we ever had to spy on anyone but now technology as well as social media has resolved these issues due to which every single individual can play as a spy at any point in his/her life although not completely yet to a significant extent.

Tracking mechanisms like bugging devices or using GPS tracking systems used to be in the access of Governments only but now even Amazon offers many tracking devices in very affordable prices. These easily accessible tracking and spying devices and

[5] PEN is an American non-profit organization with having 100 centers worldwide and they support free rights of the writers to promote freedom to express any kind of ideas, views, and opinions through literature. Currently almost 7200 writers are members of this organization. https://pen.org/

platforms has not just given rise to spying behaviors of individuals instead it has given rise to many other heinous mindsets including Harassment, Cyberbullying, Hate Speech, Online racism, Mockery etc. These technologies have provided much comfort to the stalkers/spies but less security to the victims. Initially this spying mechanism by individuals were in use to spy servants, maids, nannies and for parental controls but now this behavioral tendency has turned into something more nefarious, unethical and sometimes criminal as well. So that is how over the time of last two decades, technology and social media has manipulated the behavioral tendencies of individuals towards entirely a new yet worrisome dimension.

4.3 Role of Private Internet Companies In Mass Surveillance

Out of various internet companies e.g. search engines, cloud servers, advertisers etc. that could be a part of mass surveillance, Social Media holds the primary position because contemporary surveillance tendencies contains social media as one of the most important tool especially if the surveilling authorities have to learn about lifestyle of any individual, his/her interests, his/her family setup, his/her traveling patterns, his/her political affiliations and even what kind of personality that person holds which consequently leads to the attribute profiling of individuals along with their available forms of identity (picture, date of birth, location etc.).

Mass surveillance through social media contains many dimensions within it. It is because, there could be many different actors involved in mass surveillance through social media at different times under different conditions. That is why, while analyzing social media-oriented mass surveillance, we need to figure out some of the following aspects,

- Who is carrying it out: a government agency with certain motives which could be broad or narrow or any other party?
- Any product developer running certain business, who is interested in attribute profiling for selling its products and marketing his/her products to the potential customers?
- Any certain community of individuals?
- What kind of power relationship exists between the surveilling authority and the individuals that are being surveilled?
- What kind of data is being collected and through which means?

The answers to these questions could unveil the hidden truths about how and why social media surveillance is in progress, what is its scope and under which conditions it is being done, by using which means and by whom? Moreover, the story does not just end here instead, we need to analyze if this kind of mass surveillance is linked with cultural or political mindset or it is just being a symbol of modernization of developed nations? Or it is being used against external or internal actors during peacetimes as well as during crisis/wars? [37, p. 1118]

4.3.1 Social Media as Complicit of Government in Mass Surveillance

Either you were complicit with the project or you were the enemy of the project [76, p. 26].

The above statement highlights a very straight forward and universal fact which encompass both sides of any investigation. But we should not necessarily incline our conclusive understanding as towards something criminal, unethical, or illegal through this statement instead it presents a simple fact in case of any situation involving multiple parties. Hence, the situation itself, identities and the acts of parties involved in any certain situation can imply who is being victimized and who is the victim. This section consists of a discussion which analyzes whether social media works as a complicit to government or not and if it does, how it happens and up to which extent?

The importance as well as complicity of social media with government can be evaluated from one single fact that in the early beginnings of current decade, social media gained this much importance that it has been included in the intelligence family along with HUMINT (Human intelligence)[6], SIGINT (Signal intelligence)[7], IMINT (Imagery Intelligence)[8], MASINT (Measurement and Signature Intelligence)[9] and OSINT (Open source Intelligence)[10]. SOCMINT (Social Media Intelligence) can be defined in connection with OSINT as a source of data mining techniques (machine learning and data analysis) applied to the data collected from social media in order to characterize the behaviors of individuals under certain categories for predicting possible threats that could be posed to national security and to take measures to mitigate or counter those threats accordingly. [36]

Hence, Social Media could be a very significant actor in terms of facilitating government-oriented surveillance activities because of already having very detailed attribute profiling of masses in terms of their interests, political affiliations, educational backgrounds, family ties, thoughts etc. And that's exactly why Government has to rely on this source as well in order to enhance as well as refine the scope of data collection of their mass surveillance activities in general, but the question is under which terms and through which procedures, this cooperation happens? Next section addresses this concern in detail.

[6] It is the kind of surveillance/intelligence which is being gathered through physical and personal contact among human beings.

[7] It is the kind of intelligence/surveillance which is being done by intercepting/hacking/tapping the signals e.g. weather and communication satellites, mobile phone towers etc.

[8] It is the kind of intelligence which is being done by collecting satellite images and other collateral materials e.g. anything that is being reproduced electronically or by optical means on a film. So further analysis of such collected images refers to as imagery intelligence.

[9] This kind of intelligence is being done through the measurements obtained from different measuring and recording devices e.g. radar signals, nuclear measurements, earthquake detection devices etc. The primary purpose of this intelligence is to define the patterns and predictions regarding the on-going processes to make sure if everything is going on as per-schedule being under control.

[10] This is the kind of intelligence which is being collected from publicly available sources. Moreover, it has nothing to do with open-source software or collective intelligence.

4.3.1.1 How government establishes mass surveillance through social media?

To answer this question, Snowden's revelations can be considered as the most reliable and detailed source which covers almost every possible medium through which governments can establish mass surveillance through social media.

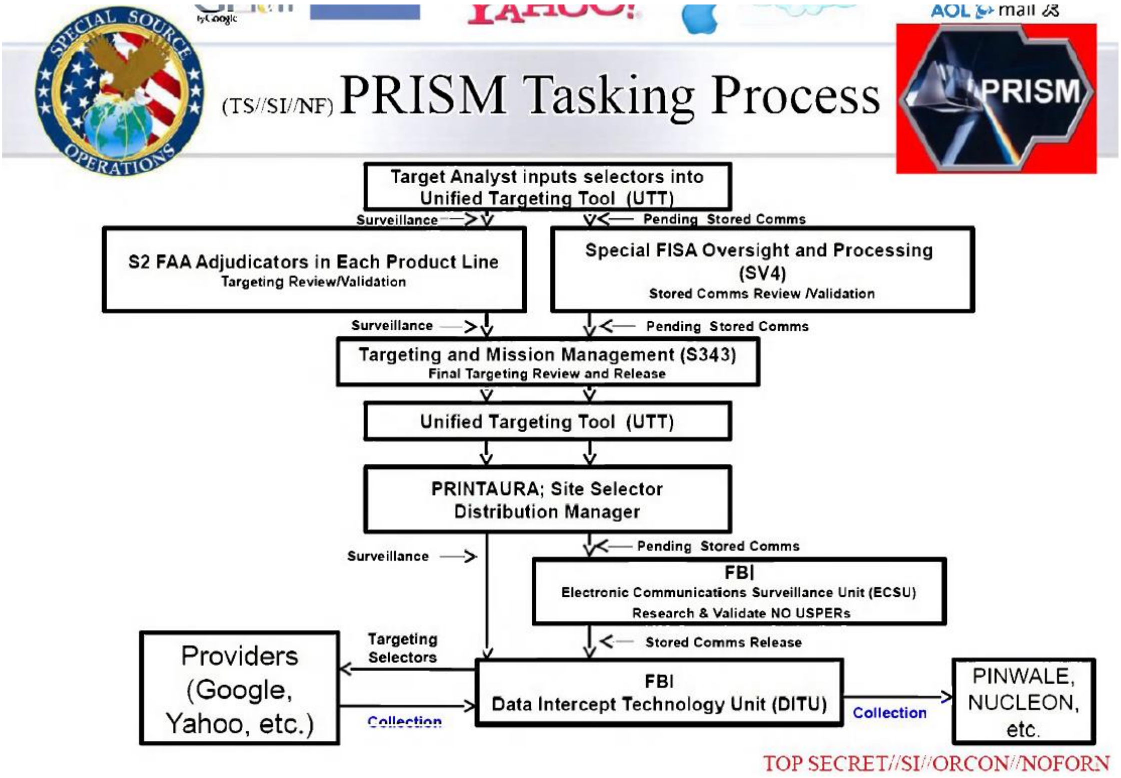
In terms of establishing mass surveillance by government through social media, search engines and more such sites, there could be two possible ways as described previously in section 3.4.2 i.e. Upstream surveillance and Downstream surveillance.

Social media is just one platform which came to limelight after Snowden's revelations but the truth is that there are many other platforms as well which are usually under the surveillance of contemporary governments which includes search engines, news websites, free file uploaders, cloud services etc. To understand how surveillance is being carried out by using Downstream surveillance mechanism, project PRISM has taken as an example which is as follows,

Project PRISM/US-984XN was primarily used as a Downstream surveillance methodology through which US government attained the collaboration of nine top internet companies which are as follows, [38, p 94]

- Microsoft (Hotmail etc.)
- Facebook
- Paltalk
- AOL (American online)
- YouTube
- Skype
- Apply
- Yahoo
- Google

Hence, the project PRISM presents a perfect scenario of how a Downstream surveillance is being carried out. It requires a special request to be made authorized by the court to the site owners and asking them for their collaboration consequently which gives an access to Intelligence Community to the content of these sites. So, it is more like an on-demand access to the data of the collaborating internet companies [39, p. 7]. And it is clearly evident from the list of the companies mentioned above that it doesn't merely includes the social media platforms instead it contains search engines and one to one communication platforms as well which really gives detailed insights about how far government could go in terms of mass surveillance. Hence, the mass surveillance done by individual companies (service providers) is just one side of the coin, while the other side of the coin unveils the connection of such service providers with the government in the name of cooperation consequently giving a free pass to government or intelligence community to have an access to the data of the users or masses. But one thing is to be noted that even in this case, the access by the intelligence community to the user's data is limited because mostly the data of specific users that are being suspected is obtained on demand from the service providers and even then, there are many intermediaries through which the approval to setup the protocol for accessing data from service providers has to be granted. Figure 3 well explains the overall hierarchy of the process through which intelligence community obtained access to user data while using Downstream surveillance especially in the case of project PRISM [40]. The format of accessing data of any individual starts from tasking request. Tasking request by any intelligence analyst for adding new target to the PRISM system automatically passes the request to the supervisor which further reviews the “Selector” or “Search Terms”.



(TS//SI//NF) PRISM Tasking Process

Target Analyst inputs selectors into Unified Targeting Tool (UTT)

Surveillance

Pending Stored Comms

S2 FAA Adjudicators in Each Product Line
Targeting Review/Validation

Special FISA Oversight and Processing (SV4)
Stored Comms Review /Validation

Surveillance

Pending Stored Comms

Targeting and Mission Management (S343)
Final Targeting Review and Release

Unified Targeting Tool (UTT)

PRINTAURA; Site Selector Distribution Manager

Surveillance

Pending Stored Comms

FBI
Electronic Communications Surveillance Unit (ECSU)
Research & Validate NO USPERs

Stored Comms Release

Providers (Google, Yahoo, etc.)

Targeting Selectors

Collection

FBI
Data Intercept Technology Unit (DITU)

Collection

PINWALE, NUCLEON, etc.

TOP SECRET//SI//ORCON//NOFORN

Figure 3: PRISM Tasking Process

Supervisor’s endorsement or belief on his/her analyst that the target is a foreign national residing inside or outside the USA’s territory is compulsory to proceed this tasking request as per the protocols. But in actual, it was not mandatory that target could only be a foreign national. It could be anyone living inside or outside American soil. Moreover, FISA (Foreign Intelligence Surveillance Act)[11] Court does not review any individual request of data collection instead it oversees the whole operation for the purpose of making legalized requests to the participating companies for data collection.

According to the tasking process shown in Figure 3, FBI (Federal Bureau of Investigation)[12] uses Government’s apparatus installed at the sites of third parties to retrieve the matching information from the participating companies e.g. Google, Yahoo etc. And then FBI passes this information to NSA without reviewing it any further. In parallel, in case of already stored information, FBI consults its own database as well to

[11] It defines, oversees, and approves the procedure of judicial requests for initiating electronic as well as physical surveillance of persons who are suspected to be involved in any kind of espionage or any terrorist activity. https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

[12] It is domestic level intelligence agency, but it is also a Principal Federal Law Enforcement Agency within USA. https://www.fbi.gov/

make sure that the new target does not matches to any previously known target or any other native American. And then as a final step, data enter in the systems of NSA in their databases known as NUCLEON, PINWALE etc. as shown in Figure 3 [41]. Here the process of data collection completes, yet the further refining is still to be done to reduce the data collection about Americans which is further shown in Figure 4 [40].

So, according to the Figure 4, the data from FBI’s intercepting units installed on the sites of private companies, is further forwarded to one or more intelligence agencies e.g. CIA (Central Intelligence Agency)[13], NSA etc. And in parallel, PRINTAURA routes the traffic flow through automation towards SCISSORS and Protocol Exploitation where the data gets segregated and stored in different databases respectively according to its datatypes i.e. Voice data is sent to NUCLEON, video data types are sent to PINWALE, call records are sent to MAINWAY and internet records are sent to MARINA. [41]

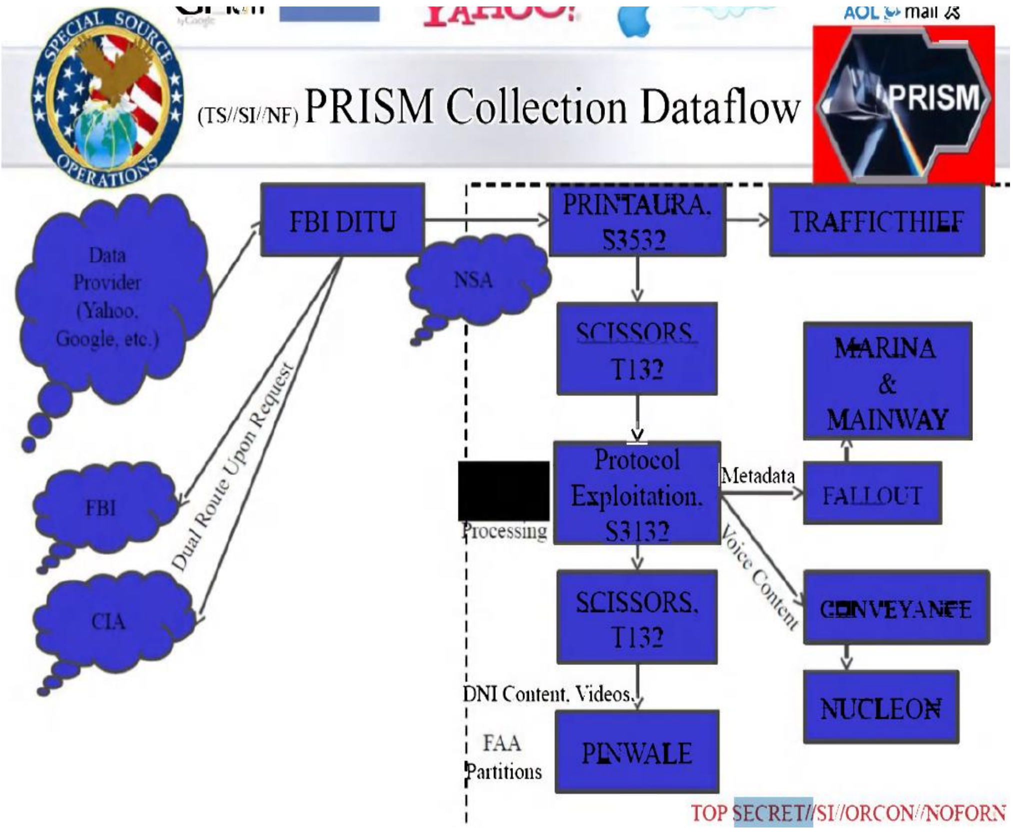
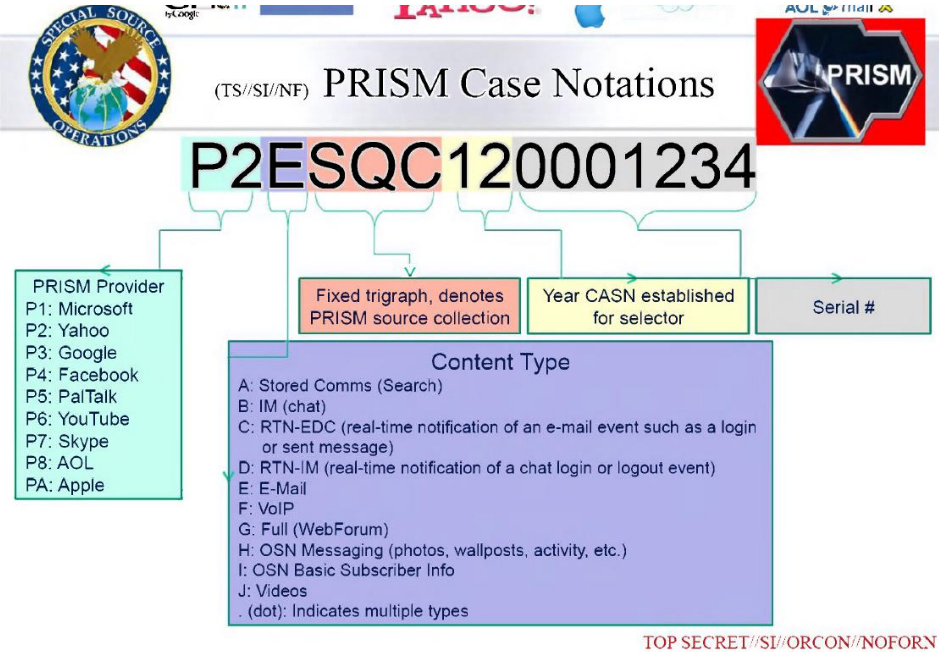


Figure 4: PRISM Collection Dataflow

The data segregation process of PRISM completes here. As it is a Downstream form of surveillance which ultimately makes it clear that there are some companies participating in this surveillance process either willingly or by court orders. The next step in this process is to monitor the target both in real time as well as through already stored data. So, for this purpose, every single target is being assigned with a unique case notation or identifier as shown in Figure 5 [40]. Figure 5 shows the rule of denoting case notations

[13] It is a Civilian Foreign Intelligence Agency that comes under American Federal Government. Its core function is to collect, process and analyze information from around the world primarily through Human Intelligence (HUMINT). https://www.cia.gov/index.html

to the targets to assign them with a unique identifier so that they could be scrutinized in future.



(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

Figure 5: PRSIM Case Notation Process

In case of Upstream surveillance, as explained above in section 3.4.2, wiretapping, hacking satellites, accessing international internet routers and using splitters in under water fiber optic cables independently as well as through the cooperation of such companies that controls the backbone of telecommunication infrastructure over which the transition of telephones and internet communication takes place are some usual methods. So, these are the typical ways which could facilitate the Upstream mass surveillance to any government agency or intelligence community. For an in-depth analysis of Upstream surveillance mechanism and how it is being carried out, case of project Upstream by NSA has been considered whose details are given below.

NSA started a mother operation by the name of Upstream which further contained many sub operations whose purpose was to access the direct and ultimate routes of the data by tapping the underwater internet cables across the US as well as internationally. So basically, Upstream can be viewed as an operation for the collection of every kind of data on the fiber optic cables that flows at the backbone or at the background of any internet infrastructure. Some of the major known projects under the head of Upstream are FAIRVIEW, BLARNEY, STORMBREW and OAKSTAR [42, p. 108].

History of Upstream data collection activities of NSA goes back to 2006 when a retired technician from AT&T revealed that in 2006, NSA installed a surveillance equipment at the AT&T's main San Francisco exchange point through which NSA was capable of collecting and analyzing every single information that was passing through that point. He further indicated that similar equipment is being installed in switching centers of AT&T. Five cities which he named other than San Francisco includes San Jose, Seattle, Atlanta, Los Angeles and San Diego [43, pp. 17-18], [44]. But experts think about it otherwise, because according to the communication experts, all these five cities are not as attractive spots for interception as many other cities could be. So, Marcus Scott (communication expert) estimated that AT&T has 15 to 20 splitter sites across USA [44]. Figure 6 shows an estimated mapping of splitters across different cities of USA. The map was made based on tracking the traceroutes of major chunk of internet traffic within USA [45]. This program was called as "Warrantless Wiretapping" by James Bamford[14], which was later on officially changed to "Terrorist surveillance program" (TSP) by Bush administration [46, p. 289].

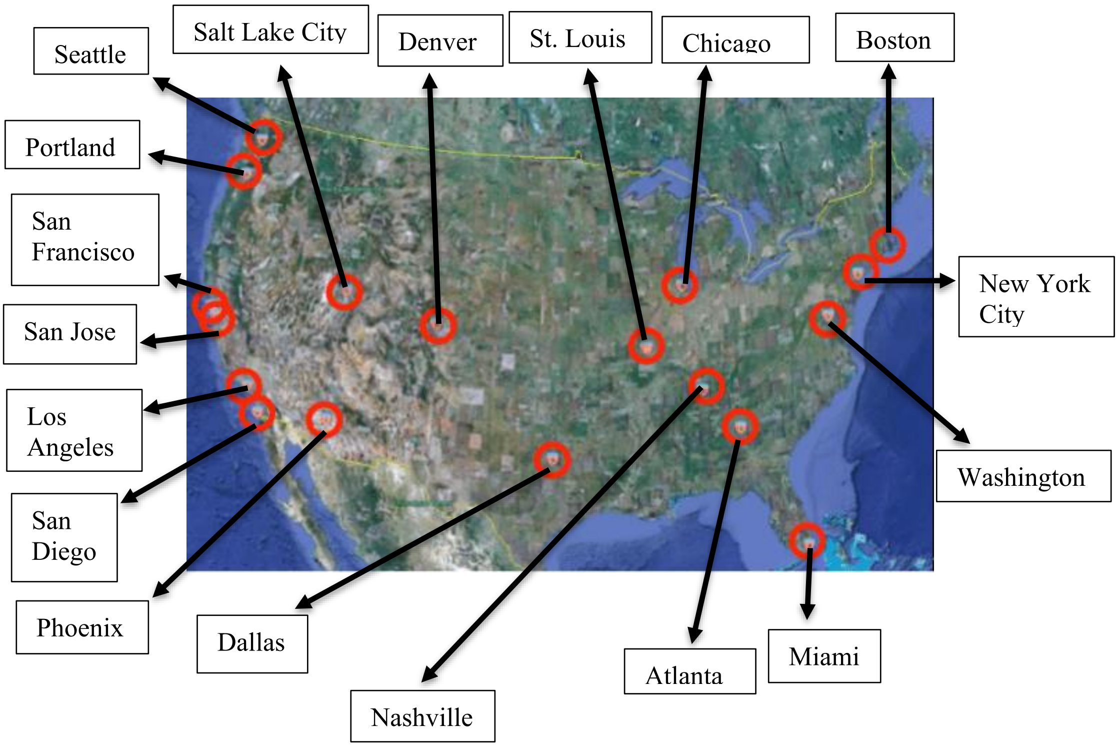


Figure 6: US Cities having Splitters by NSA

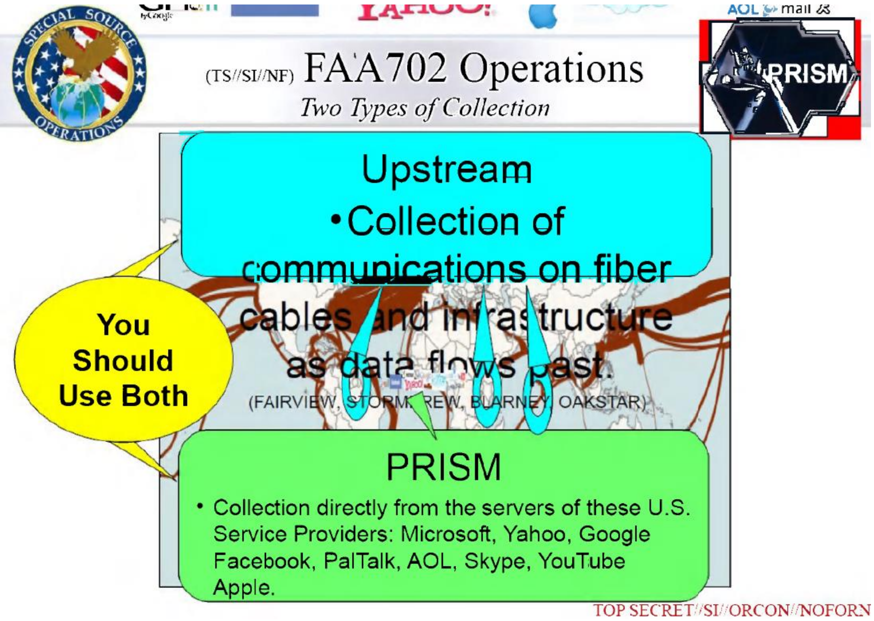
Figure 6 represents 18 US cities having high likelihood of having splitters deployed by NSA. The list includes Nashville, New York, Chicago, Atlanta, San Jose, San Diego, Dallas, San Francisco, Seattle, Miami, Phoenix, St Louis, Denver, Salt Lake City, Washington, Boston, and Portland [45]. Up till this point, that upstream mass surveillance remained as confined within domestic boundaries but later it expanded.

Upstream data collection was primarily designed for bulk data collection and it proved to be the most significant yet challenging mode of surveillance as it required a physical access to the internet's backbone infrastructure including under water fiber optic cables and internet routers/switches. Even after the revelations made by the Snowden in June 2013, very few details came up to limelight regarding Upstream. Despite this fact, leaked documents about Upstream appears to present two methods for bulk data collection which are as follows,

[14] James Bamford is America's Best selling author, documentary producer and a journalist as well. He is famous because for his extensive research work on American Intelligence agencies especially on NSA.

1- Installing fiber optic splitters with major internet switches.
2- And where the switch operators did not cooperate, NSA took a more challenging route in which they physically tapped the cables themselves under water somewhere along the route between the switches. [44]

Majority of the internet travels through underwater submarine cables so it certainly indicates that either NSA installed the wiretapping mechanism somewhere near the shores or might be somewhere in the oceans deep below. In both the above stated methods, DPI (Deep Packet Inspection) was used to store and analyze every aspect of data including both metadata and other communication content (packet payload). In this kind of interception methods, data is mostly obtained in a distorted format, that is why it must be reassembled before any further analysis or any other kind of usage [44].



(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

•Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

• Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

Figure 7: Upstream and PRISM (Sub Operations)

Figure 7 shows a training slide from one of NSA's program named PRISM, but it shows Upstream as well [44, Fig. 5]. This slide is obtained from one of the top secret documents leaked by Snowden and this slide shows some submarine routes of fiber optic cables at the background and summarizes the motive of Upstream data collection operation as "Collection of communications on Fiber Optic Cables and infrastructure as data flows past". And it has further mentioned the sub-projects of Upstream as well in the brackets i.e. FAIRVIEW, STORMBREW, BLARNEY and OAKSTAR. [40]

While moving towards the completion of Upstream data collection operation, it is important to understand the main theme of the four sub-operations under the head of Upstream. This understanding will help us to figure out how responsibilities of tasks were distributed in different phases and through which sources. The description of all these four sub-operations is as follows,

1- **FAIRVIEW:** This program was responsible for producing DNI (Digital Network Intelligence)[15] reports. Its scope was confined only within USA and it used to filter almost one million emails a day. It was operating in close collaboration with FBI. [47]
2- **STORMBREW:** This program was operating on global level and its architecture was based on QRC (Quick reaction capability) systems and it was responsible for providing critical intelligence for Global war on Terrorism. [47]
3- **BLARNEY:** This was more of a data collection portal which was responsible for providing leverage to intelligence community and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks [48]. Moreover, the team of this program worked to enable the UN security council's data collection as well [49]. Under this program, NSA also gained access to complete and more detailed content of Facebook users unlike downstream surveillance (PRISM) [50].
4- **OAKSTAR:** This program was further subdivided in more branches. The most important branch of this program was ORANGECRUSH whose purpose was to forward collected metadata to the third party which was primarily Poland at that time. That metadata included the data of Afghan National Army, Limited African Continent, Middle East and even some of the European communications. [51]

To visually demonstrate the difference between Upstream (FAIRVIEW, STORMBREW, BLARNEY & OAKSTAR) operations and Downstream operations (PRISM), Figure 8 represents a complete view containing all the necessary hierarchies and connections from top to bottom [52].

Figure 8 presents a very detailed view of the mass surveillance established by NSA right from the base of communication cables. Then it shows all the nine service providing internet companies that were willingly or compellingly involved in bolstering the mass surveillance activities of US intelligence community. Figure 8 represents one very important point to be noted that whether it's the case of upstream or downstream surveillance, intelligence community needs to go through some sort of legislative formalities or legal protections in order to stage the fact that every operation is being done within legal boundaries under the supervision of legal authorities or even if it's illegal, then immunity must be granted in advance to make sure that there will be no consequences whatsoever. This implies that there are some laws available which oversees such programs but about the adherence of those laws, there are no clear evidences. But one thing is evident that before executing any kind of mass surveillance operations, intelligence community must obtain the approval from some judicial authorities. Hence, as shown in Figure 8, from legal perspectives, it appears that the surveillance programs needed to be approved by two judicial authorities i.e. Section 702 of FISA Amendment Act (FAA) and Section 215 of the Patriot Act. The former one allowed the execution of PRISM operation in general while the latter one allows the intelligence community to work in collaboration with the telecom and internet companies for obtaining any kind of records of any individual and both these Judicial

[15] This term is specifically used in American Intelligence community which implies the intelligence that is gathered by intercepting digital communications transmitted between networked computers.

Acts altogether actually facilitated the upstream as well as downstream mass surveillance operations.

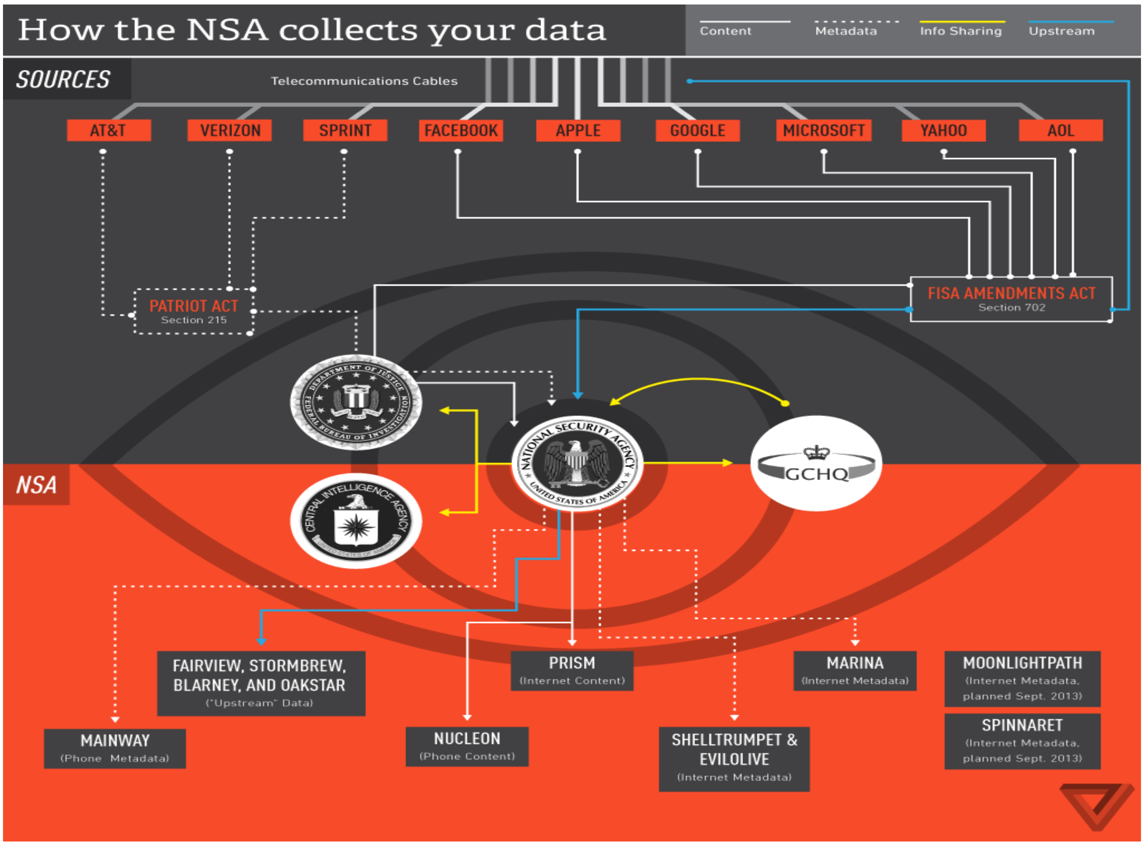


Figure 8: NSA's data collection process

Moreover, through the documents leaked by Snowden, one more aspect came to limelight that FISA created a secret court by the name of FISC in order to insidiously oversee the mass surveillance targets both domestically and internationally [53], [54].

The analysis of PRISM and Upstream clearly satisfies our claim that we made in Chapter 3 implying that mass surveillance is always based on four variables i.e. scope, methodology, quantum of data and type of data. PRISM represents the scope of mass surveillance on domestic scale with the targeted data collection, while Upstream and its sub-operations represents an international scope of mass surveillance which involves targeted as well as bulk data collection along with metadata as well as content-specific data collection.

4.4 Governments Involved in Mass Surveillance Across the Globe

Contemporary mass surveillance by any Government across the globe cannot possibly be executed without involving any third parties or more precisely, privately operating organizations because internet has become the primary source of executing mass surveillance activities. But because of the enormous, rapidly expanding, and perplexed nature of internet, it is not practically possible for any individual government to execute such activities solely on its own. And this is what compels the governments to rely on third parties directly or indirectly and that is what necessitates the presence of third parties in the surveillance architecture in any part of the world established by any government. There are six different categories of such third parties based on their functionality which are as follows [73, p. 17],

1- ISPs/Telecom Service Providers.
2- Underwater Fiber Optic cable providers.
3- Vendors providing telecommunication Network equipment.
4- Companies developing or selling surveillance technologies including both software and hardware platforms.
5- Contractors of Military and security companies operating privately.
6- Partners or distributors of companies manufacturing surveillance technologies.

Edward Snowden is the living example of this collaboration bridging government and private organizations in terms of surveillance because he himself was a contractor of a private consulting company by the name of Booz Allen Hamilton [73, p. 14]. This company provides solutions in terms of analytics, engineering and cyber-security which ranges from health to defense to energy and to international development [74].

According to the data collected by Privacy International in their report of 2016, there are about 528 companies that are providing surveillance services to various governments across the globe. Out of which USA, UK, France, Germany, and Israel holds the title of having the highest number of surveillance companies within their borders, respectively. Similarly, while analyzing EU, there also comes five countries which tops the list in a descending order respectively i.e. UK, France, Germany, Italy, and Czech Republic. And the countries having lowest number of surveillance companies includes Bulgaria, Croatia, Cyprus, Estonia, Greece, Malta, and Slovenia. Belgium holds the position of a country with second lowest number in this regard with having only two companies. While Finland, Lithuania and Hungry each contains three surveillance companies within their borders [73, p. 19]. So, that is how the surveillance architecture across the globe has been established by various governments in collaboration with privately operating surveillance companies. Now the point here is that whether such governments are merely involved in surveillance related to individuals or they have established infrastructure based on all-seeing eye just like a Panopticon? The answer to this question could be shady and unclear because this is something needs to be dig down more by analyzing the activities of every single government individually. But having surveillance companies within the borders can facilitate any government to have small-scale as well as large scale mass surveillance depending upon their tendencies. But we cannot weigh all such governments in a same scale by declaring all of them as doing something unethical, un-consensual or insidious because mass surveillance is not only being done in order to spy over the masses instead there could be many other purposes as well out of which voting systems, public data analytics, population register analysis, tax records etc. are also the activities that requires mass surveillance. Hence, USA is not the only government that was ever involved in mass surveillance activities instead various governments across the globe can be seen being inclined towards this tendency in which China, Japan, Russia, and Israel tops the list.

4.5 Advertisers, Product Developers and Data Collectors

Social media presents merely one class of private internet companies whereas there are many other categories as well in this regard which are involved in surveillance activities individually as well as collectively. This section addresses IT companies other than social media, their ways of working and methods through which they achieve their surveillance requirements.

We are living in a digital era where user privacy has become a commodity that is often bought, sold, sorted out and being used in many different ways which could include surveillance, attribute profiling, data analytics, advertisements and so on and so forth. That's why user data has become an important asset for IT companies which are further linked with advertisers as well as with data trackers for maintaining a very precise and anonymous mode of trading and tracking mechanism among each other mostly without the information of users. Consequently, web companies, data trackers and advertisers try to gain a competitive advantage by collecting as much data as possible about the users which later results in their detailed profiling for the purpose of sale and purchase to other companies. That data is primarily based on the interests, geolocations, preferences, personally identifying information of the users as well as their mode of using internet which is being sold and purchased for various motives which are usually out of the approach and control of the user. This race of data collection urges web companies to develop more and more precise methods for tracking users across the internet in which cookie collection method is the most traditional, useful, and insidious one. Cookies collection method is based on maintaining some sort of state at the client's side whenever he/she visits any site and then that state would be used to detect that same user across different domains and sessions. There used to be two types of cookies initially i.e. 1st party cookies and 3rd party cookies. 1st party cookies were supposed to record the user's data whenever any user visits the same site repeatedly by maintaining state at the user's side. While 3rd party cookies were later developed to track the same user whenever he/she hops from one website to another. Cookie based detection method is also known as storage based data collection method and it's so invisible that whenever any cookie by any server is being stored or read from the client's system, the browser doesn't pop-up any notification. Moreover, it does not even require any kind of interaction between the user and the server. Cookies can be stored by the server at client's side via using two methods, i.e. through JavaScript by using API (Application Programming Interface) call or through HTTP responses which contains the Set-Cookie header. Similarly, these cookies can be read by the domains/servers in two ways as well, i.e. they might be directly attached with the automatic HTTP request made to the domain with which the cookies belongs to via Cookie header or in other case, they can be explicitly called by the JavaScript API and then they are sent to the server [55, p. 156].

To curb this data collection by data trackers and advertisers, Same-origin policy was invented few years later, whose primary purpose was to limit the amount of data third parties could collect about the users. SOP proved to be quite a hurdle for ad-industry, data collectors and other web companies, because the core functionality of SOP was to make sure that if a user is viewing any webpage on his/her web-browser then the script running on that webpage should be able to read and write from any other web page if and only if both webpages have same origin. Origin can be defined as something made up of three components, i.e. Application layer protocol of the page (HTTP or HTTPS), TCP port number of the webpage (80 or 443) and domain name of the webpage (e.g. www.facebook.com) [56, p. 151]. Therefore, to overcome SOP, these 3rd parties invented Cookie Synchronization mechanism also known as Csync [57]. Csync is basically designed to bypass or to deceive same-origin-policy. Csync allows different web companies to share the cookies and to match the IDs (Identification) of the same user by collaborating with each other's script to track the same user whenever he/she hops from one website to another.

Hence, the primary motive of all such companies is to collect as much data as possible and as much precise data as possible so that further operations could be performed on them. Such companies usually do not work as a complicit to governments instead they have their own market and economics around which their activities revolve and generates capital. Such companies doesn't have the motive to specifically victimize or track any certain individual in order to pre-detect any possible threats on national or international level unlike governments instead such companies are solely concerned with data collection and its sale-purchase. But yes, such companies intend to track as many individuals as possible for the purpose of collecting, sorting and analyzing their data which consequently bring such companies as well in the list of actors involved in mass surveillance irrespective of their purpose whatsoever. Just like social media and governments have certain ways of tracking masses around the internet, these companies also have some tracking mechanisms for the purpose of data collection. The next section addresses their primary tracking mechanisms of surveillance in detail including cookies.

4.5.1TrackingMechanisms

There could be many possible techniques that can be used to track the users both individually as well as collectively. Many of them have been already discussed above in this chapter. Methods discussed above implies a very refined and organized form of mass surveillance mainly setup by governments and social media. But this chapter also aims to highlight some of the methods that shapes the core of the tracking infrastructure established by Internet Companies such as product developers/manufacturers, advertisers, and data collectors etc. The user tracking mechanisms discussed in this chapter presents both the consensual as well as non- consensual, hidden as well as public and active as well as passive modes of tracking. Out of many such methods, Cookies and Fingerprinting along with various types are the ones that holds the prime importance in bolstering the tracking topologies of private internet companies. Governments and private internet companies may or may not necessarily be linked with each other but majority of the private internet companies from different sectors are mostly linked with each other because their inextricable connection with each other forms the core of their business infrastructure consequently driving the economics of their business activities. That is why their aim is always to achieve as much centralization as possible in terms of developing user tracking mechanisms which further depends upon the kind of business activities they have.

4.5.1.1 Cookies:History & Background

The foundation of communication among people living in far-off areas from each other was laid back in 1960s. At that time, the purpose was primarily to connect scientists who were living at distance from each other. So, basically, the forefathers of internet did two things in 1960s, first they opened secure communication channels for the scientists living in far-off areas from each other and secondly, they managed to enhance the efficiency and speed of information exchange and connectivity [58]. But precisely speaking, contemporary internet has been still doing the same since then, but not as securely or as privately as it used to be initially. Introduction of cookies has entirely changed the meaning of security and privacy on internet and it has affected both factors to a significant extent which further gave rise to many other insecurities as well as vulnerabilities to the user's information.

The history of cookie's introduction is much more concise than the history of internet. Before the invention of cookies, the communication that used to take place between the user and the server was anonymous because of having no intermediary recording, tracking or surveilling mechanism in between other than a communication medium whose sole purpose was to maintain a connectivity between the user and the server. But the introduction of cookies back in 1994 perished the user's privacy entirely by changing the earlier scenario of anonymous communication between user and any remote server.

A guy Lou Montulli[16] introduced a piece of code written in HTTP (Hypertext Transfer Protocol) based language i.e. HTML (Hypertext Markup Language) by the name of HTTP cookies. Initially, it was labeled as *State Information* during the filing of patents in 1995 and was defined as a mechanism which could be used to tackle the memory loss in data exchanges. Later, in 1998, the company named Netscape where Montulli was working got a patent (Patent number: US5774670 A) and his invention was awkwardly declared as "Persistent Client State in Hypertext Transfer Protocol Based Client-Server System". So, according to the invention of Montulli, now this newly introduced mechanism was able to store the information on user's computer about the transaction or information exchange that takes place between the user and any remote server and this information could be retrieved at a later date. [59]

It cannot be said precisely, that what were the intentions of Montulli or the company in which he was working or the authorities which granted him the patent back in 1998, but this can be clearly understood that Montulli's invention opened the door to a never ending quest of security and privacy among the users and the internet companies because the story didn't end here as it further gave rise to different web-tracking technologies on internet which are still in practice till date. Because the cookie's invention didn't just introduce a storage mechanism of the user's state during internet surfing instead it gave rise to tracking mentality which kept on changing forms and converted into different forms of surveillance which have deeply penetrated in current networking infrastructure globally, consequently putting user's privacy at risk and whose details can be seen in upcoming sections.

[16] http://www.montulli.org/lou

4.5.1.1.1 How Cookie Synchronization(Csync) works?

In order to understand the cookie synchronization mechanism, there is a Figure 9 given below which represents how the cookie synchronization mechanism works and how it brings the sense of more connectivity and centralization among the owners of different internet companies which involves data collectors, product developers and advertisers as well. Before the development of Csync, all the advertisers, product developers and data collectors were connected anyway, but that kind of connectivity had to go through a very complex procedure which consequently added extra consumption of their resources in terms of their data collection, segregation and processing capacity but after the development of Csync, this extra consumption has been reduced to a significant level consequently providing a kind of automated tracking mechanism which not just collects data instead it keeps the different internet companies linked together through collaboration and centralization in terms of their tracking mechanisms.

Figure 9 presents an easy to understand example for explaining the working mechanism of Csync methodology [57, Fig. 1].

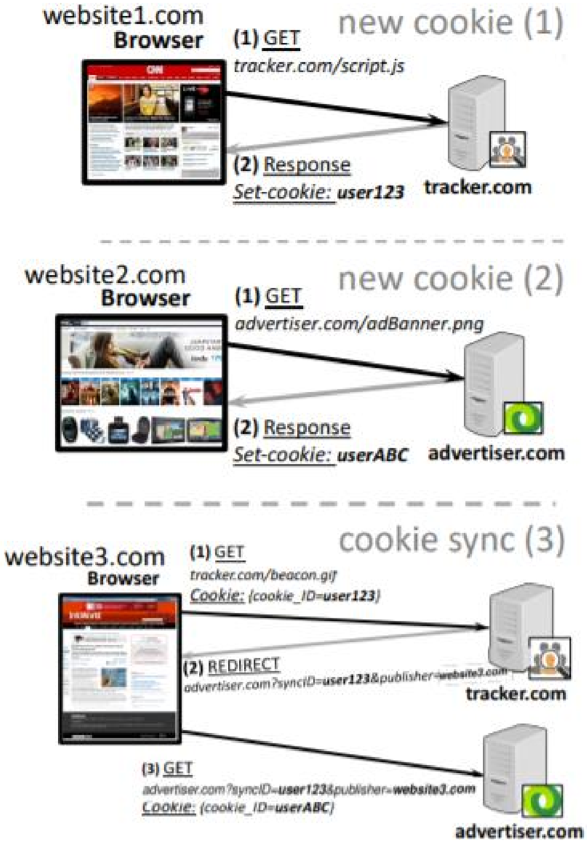


Figure 9: CSync Process

Let us just say a random user visits two different websites by the names of website1.com and website2.com, where there are some 3rd party trackers e.g. advertiser.com and tracker.com. So, now these two third party trackers can set their own respective cookies to identify this same user in the future. So tracker.com assigns the identity to user as user123 and advertiser.com assigns the identity to that same user as userABC. So, both the advertisers know the same user but with different identities. Let us assume that same user visits third website by the name of website3.com which contains some sort of JavaScript from tracker.com but not from advertiser.com. So, currently for advertiser.com, this user is new but not for tracker.com. That's why when the code of tracker.com is called, it initiates a GET request to the browser by tracker.com as a step.1 and in step.2, it responds back as REDIRECT request which instructs the browser to issue another Get request to the collaborator of tracker.com which is advertiser.com and it happens through a specifically designed URL (Uniform resource locator). So, when advertiser.com receives this request along with cookie Identity userABC, it finds out that this userABC is visiting website3.com. This whole procedure leads to the identification of one more important thing which is that the user known to tracker.com as user123 is the same userABC which is visiting website3.com. That is how Csync facilitated advertiser.com to collaborate with tracker.com to find out which user visits website3.com so that both tracker.com and advertiser.com could synchronize the different identities of the same user while he/she visits different websites [57]. This whole process gives entirely an unauthorized access to data tracking and advertising companies over the information of users which centralizes the tracking mechanisms of third parties through synchronization as well as collaboration.

Cookies synchronization is just one basic method which is under the use of many data trackers, advertisers and social media owners while in parallel, there are many other techniques in practice going on in order to obtain the most precisely possible data collection highlighting the most detailed attributes of the users across the internet.

4.5.1.1.2 Types of Cookies

Cookies are usually divided in many types depending upon their mode of operation (storage and reading mechanism) and their expiry dates and many other attributes as well based on which cookies can be categorized [60]. The concept of 1st party cookies and 3rd cookies described in section 4.5 describes two generalized types of cookies which are primarily based on two factors, i.e. tracking the frequency of the visits by any user on a same domain and tracking that same user across different domains respectively. Similarly, cookies can be differentiated based on their expiry dates as well. So, based on their lifespan, cookies are divided in two types i.e. session cookies and persistent cookies. Session cookies expires the moment user closes the browser while persistent cookies remain stored for longer period which further depends upon their sub-types and the server of those cookies which has stored them at client's side. Following are some types of the cookies based on their different attributes including their mode of operation and expiry dates.

- HTTP cookies.
- Flash cookies.
- Local Connection Objects of Flash.
- Super Cookies/ Ever Cookies.

4.5.1.1.2.1 HTTP Cookies

HTTP cookies are the general first-party cookies (as explained above) which are stored by the domain at client's side merely to monitor the same user from same browser. It primarily identifies the returning user within the same domain. But these first party cookies operate in combination with some other modes as well which are as follows,

1- **Connecting explicit Web-form authentication with cookies:** This method involves in combining the web-form authentication mechanism and cookies together. What happens in this method is that whenever a user visits a certain domain, the domain asks that user to get him/herself register on this website to access the content of that domain. So, in this way, the content of the website becomes available to that user only who logs in to the website by using his/her credentials. This kind of tracking mechanism is independent of the browser, computer or even the location from where the user has logged in [60]. This method provides quite a leverage to the server to record the activities of the user apparently in a so-called consensual way.

2- **Cookie Leakage/Synchronization:** As explained above in section 4.5.1.1.1, apparently it uses the first party cookies for executing this methodology, yet it connects the user with third parties because of cookies synching mechanism which allows different website owners to track the same user whenever he/she visits any such site which contains the scripts from their collaborators. E.g. If a user visits website of Amazon, then his/her cookies from the domains of collaborators of Amazon will also be stored in the system of that user because of the collaboration of Amazon with other third parties by having their script on Amazon. So, in this way, they can be called as third-party cookies as well and such cookies are primarily used by data trackers as well as advertisers to track the same user across different websites.

3- **Advertisers and trackers:** Some domains contain certain number of data trackers embedded in them which helps in aggregating the tracking services through cookies. E.g. a tracker by the name of ameld.com is well known for making requests to other data trackers, and the request contains the websites visited by a certain user and the unique identifier assigned to that user by the aggregator [60].

4.5.1.1.2.2 Flash Cookies

These cookies are stored by the Adobe Flash plugin and these are much more difficult to control by the user because these kinds of cookies never get stored in the same memory as HTTP. These cookies are primarily used for providing smooth streaming experience on multimedia websites. These cookies are also known as LSO (Local stored objects). Moreover, these cookies can also retrieve even the deleted cookies [61]. Flash cookies can be stored up to the size of 100kb which is much more than the HTTP cookies as it merely stores up to 4kb, so in this way, Flash cookies are able to retrieve much more information than conventional HTTP cookies. They are accessible from all the browsers installed in the same system so that is why the user can be tracked irrespective of the browsers within the same system. Moreover, Flash cookies also do not expire by default [60].

4.5.1.1.2.3 Local Connection Objects of Flash

The local connection objects of Flash are used to create an interaction between different SWF (Small Web Format)[17] files running in the system at the same time, which consequently makes these objects to communicate with each other even during the instances running between normal window and private window. These objects combined with Flash cookies can even pass values from cookies of the normal browsing window to the Flash instances that are running in a private browsing window [60].

4.5.1.1.2.4 Super Cookies/Ever Cookies

As explained in Flash cookies, that such cookies can be respawned even after deletion and this is what makes them called as Super cookies or Ever cookies and such cookies fall under the category of persistent cookies. Super-cookies are being constructed through JavaScript by using various forms of storages in the browser which includes HTTP cookies, LSO of Flash Cookies, Silverlight Isolated Storage, Web/browser History, Etags, Window.name DOM property, Web Cache, User Data storage of Internet Explorer, HTML5 storage (Local, global and session), HTML5 Databases and few other attributes from JavaScript [60, p. 13]. From this retrieval mechanism of deleted cookies, one can easily imagine the extent up to which this tracking mechanism can go through and how deeply these cookies has been rooted in our systems and how near to impossible it is to get rid from this kind of surveillance by a normal internet user at least being on surface layer of the internet (Refer to section 1.2.1).

Other than these above four types of cookies, there are many other types of cookies as well which includes [60],

- ➢ Silverlight Isolated Storage.
- ➢ HTML 5 Global, Local & Session Storage.
- ➢ Web SQL Database and HTML5 Indexed Database.

For awareness, every single user who wants not to get followed across the internet through cookies needs to cross the following hurdles which are as follows [61],

1- A user needs to find out the appropriate method or settings that could allow the sites to use/store only the necessary kind of cookies merely for user interface but prevents the cookies that involves tracking.

2- A user needs to educate him/herself about all kind of Super-cookies including the hideous ones as well and then need to find settings or additional assistance through software or scripts which could disable the Super-cookies. And precisely speaking, for an average user it is not something easy to do.

[17] These are the kind of file formats which are primarily used to display animations on any website. SWFs are always created by Adobe Flash and such files can't be edited, because for the purpose of editing, we need to obtain original flash file having extension of .fla.

An average user might pass first hurdle successfully after having enough research on cookies and how to disable, delete them permanently or limit them but the second hurdle needs advanced knowledge, skill set and awareness. Even if a user crosses both these hurdles, there is still a third hurdle waiting ahead which is known as "Fingerprinting" or just "Device Fingerprinting". Cookies itself cannot be tagged as something intrusive, dangerous, or even a threat instead the way they are being used by internet companies is something that invades an individual's privacy. We cannot even call them spywares because the text string or the code in them is not executable at all [95].

Device fingerprinting is also a kind of tracking mechanism but the worst part about this technique is that it does not involves any kind of visible storage state or running script which could be blocked, deleted, or could be limited. Even a user who gets able enough to develop a control over Super-cookies of his/her own system might not be able to tackle this situation or to pass this hurdle, because this tracking mechanism in most cases leaves no visible or persistent trace on the client's side which makes this mechanism hard to be tracked due to its insidious nature. This tracking mechanism is explained in next section. Moreover, this mechanism can extract way more detailed information than cookie detection mechanism.

4.5.1.2 Fingerprinting (Cookie-less Tracking)

Cookie detection mechanism is not the only way to track any user by the web companies instead there are many other methods which involves cookie-less tracking methods, and Fingerprinting is one of them. But fingerprinting cannot be described as an individual methodology instead it consists of group of methods bind together for performing a common function which is tracking or surveilling the users across the internet without having the support of cookies due to which it can also be called as stateless web tracking. In case of cookies, every individual user has a unique but same identifier which is being used across every single website he/she surfs, while this does not happen in case of fingerprinting. In fingerprinting any single user can be tracked across different websites having different entities which is not possible by using cookies [60].

In case of fingerprinting, neither any cookie is being generated nor the user needs to log in for accessing the content of the domain, and this method is also independent of the fact that whether the browser accepts the cookies or not. That is exactly why a user cannot find out if he/she is being tracked or not and how he/she can prevent this tracking mechanism. There can be a way out of this situation by turning off the support of JavaScript, yet it will only block the active fingerprinting but not the passive fingerprinting. [60]

Browser fingerprinting can be defined as,

"*A browser fingerprint is a set of information related to a user's device from the hardware to the operating system to the browser and its configuration. Browser fingerprinting refers to the process of collecting information through a web browser to build a fingerprint of a device. Via a simple script running inside a browser, a server can collect a wide variety of information from public interfaces called Application*

Programming Interface (API) and HTTP headers. An API is an interface that provides an entry point to specific objects and functions. While some APIs require a permission to be accessed like the microphone or the camera, most of them are freely accessible from any JavaScript script rendering the information collection trivial". [62]

Generally, fingerprinting is divided into three types based on its sources through which it operates i.e. Active, Passive and Cookie-like Fingerprinting. All three types are further subdivided based on the target information and the techniques used for execution.

- **Active Fingerprinting:** In this case, the site runs some sort of JavaScript or any other code at the local client in order to extract more detailed information about the user including information about the additional characteristics of browser, device etc. [63]
- **Passive Fingerprinting:** This kind of fingerprinting is based on extracting the information through the observable characteristics in the contents of the Web request without using any kind of code or script at the client's side. This type of fingerprinting usually extracts the information about the browser and its version, operating systems etc. [63]
- **Cookie-Like Fingerprinting:** This type of fingerprinting is primarily involved in re-identification of the state that is first set or stored by the user, user agents or devices and could be retrieved later. Cookie-like fingerprinting works in a same way as HTTP cookies works to re-identify the stored state of the user. Moreover, this type of fingerprinting also prevents users to remove or limit the cookies stored by the user agent just in the case of Ever-cookies (See section 4.1.1.1.2.4) [64, pp. 9-23]. That is why this type of fingerprinting can track the users even through the stored states across devices, browsers, and software upgrades unlike active and passive fingerprinting [63].

Beside the types of Cookies and Fingerprinting discussed above, there are few other methods as well which are in practice with web companies, hackers, social-media giants and government organizations in order to quench their thirst, need, want or may be habit of surveilling masses, e.g. [56].

- Session identifiers.
- Clickjacking.
- Embedding identifiers in cached documents etc.

Covering all the types of cookies, fingerprinting and every single possible tracking mechanism under practice regarding mass surveillance will lead us out of the scope of the actual topic of this thesis. The cookies and fingerprinting discussed above in detail are the ones that are included in most used tracking mechanisms by various web-companies, data trackers and advertisers. That's why only up to intermediate level, both Cookies and Fingerprinting techniques have been explained so that the overall idea behind the surveillance/tracking mechanism through both of them could be understood, otherwise internet Cookies, browsers, Fingerprinting and JavaScript are whole different topics which requires completely a separate and dedicated research work.

Chapter 5: Ethics & Mass Surveillance

Ethics is a branch of philosophy which deals with formulating certain code of conduct which further defines some standards for declaring any act as morally right or wrong. And all such codes must be acceptable for all the people or at least by most of the population under consideration. The word “Ethic” defined by Cambridge dictionary is “A system of accepted beliefs that control behaviour, especially such a system based on morals”. And “Ethics” is defined as “The study of what is morally right and what is not” [1]. Different theories have been presented to define as well as explore ethics from every possible dimension in which most famous ones are known by the names of Utilitarianism, Rawlsian, Kantian etc.

This chapter addresses ethical analysis of Snowden’s act of revelations, top three accusations posed on him by US government and mass surveillance through the lens of Utilitarian thinking. This chapter also presents justification behind the choice of Utilitarianism as a base theory for ethical analysis.

5.1 Cyber-Ethics

As a self-explanatory terminology, we can assume that study of ethics related to cyberspace is called as cyber-ethics. Cyber-ethics are related to the study of information over the networks and the computers, its impact on users and the way it is being used [2].

Therefore, cyber-ethics are aimed to make sure that all such computer/network/internet-oriented activities are being executed in morally acceptable ways. Similarly, different philosophers and researchers have explained and defined cyber-ethics in different ways but all are agreed at one point when it comes to the standardization of cyber-ethics, and that is the morally valid and acceptable framework of norms related to cyberspace. Cyberspace represents a metaphorical implication of an imaginary space that exists within the scope of internet while internet represents a global network which is made up of numerous smaller networks, computer, and servers. Therefore, using cyberspace ultimately implies internet in our discussion.

5.2 Choosing an appropriate Ethical theory

Choice of an ethical theory can be varied from situation to situation, but a pre-analysis of ethical philosophies in general can significantly support us in choosing the most appropriately fit ethical theory. Choosing an ethical theory primarily relies on how we define good or morals? Hence, to define what good means to us will eventually compels us towards normative ethics. It is always a cumbersome task to find out that which normative theory fits exactly in any certain situation, yet this thought process usually proves as quite an eye-opener and an exploring journey of behavioral philosophies from multiple dimensions. So, in this regard, there are generally three school of thoughts which can help in preliminary generalized categorization of ethical theories. Hence, we can either be Virtue theorist, Principle-Based theorist, or Consequence-Based theorist.

If we are a virtue theorist, we primarily emphasize on one's personal character to judge the morality of his/her actions. So, in this view, people rely on their self-esteem to drive their actions which consequently constructs a base understanding of their beliefs in terms of morals. E.g. if a person plagiarizes any material which later on gets detected by his/her peers or seniors, and they know him/her very well that he/she is a person of good character and he/she follows rules and regulations, then they might become slightly lenient in judging him/her irrespective of the fact that plagiarism is a crime. The judging authorities would also try to draw positive conclusions about the researcher's plagiarized work while judging him/her so that he/she could have a leverage of his/her good character consequently preventing adverse effects on his/her grades during academic evaluation. Conversely, a person already notorious with reputation of academic misconduct would not be able to avail this leverage in case he/she commits the same crime. Majority of the virtues theorists are inspired from Aristotle because he proposed that virtuous person is the one who has ideal character traits. Although the list is quite long, but some of the most famous virtue theorists includes Elisabeth Anscombe, Bernard Williams, and Alasdair Chalmers MacIntyre.

Being a believer of Principle-Based ethical approach, we always rely on some generalized principles that are pre-implemented in our surroundings e.g. religions and cultures always promulgate some hard-coded set of rules to guide the behavioral tendencies of masses both on individual scale as well as collectively and that's how the morality of any action is being translated into good or bad by considering those principles as a parameter of judgement. This kind of belief is known by the name of Deontology. And it solely relies on following universal principles e.g. do not lie, do not cheat, do not steal etc. This can best be explained with a following example i.e. There is a cyber-security specialist who comes to know that a nuclear missile is about to be launched that would start a war and thousands of innocent lives will be perished in few moments, so if he hacks the network of his/her own nuclear facility and prevents that launch, it will make his/her act as unethical according to deontology because breaking into someone's network without permission implies lying, stealing and cheating irrespective of the fact that his/her intention was to save thousands of innocent lives. Hence, deontology is all about following hard-coded universal principles irrespective of their consequences. Deontology dates to Immanuel Kant (1724-1804). He had the idea of rejecting anyone's subjective experience in terms of ethics instead there should be an irrefutable set of rules and logics which could translate the morality of any action. John Rawls is another famous name in this regard.

Virtue ethics and Principle-Based ethical beliefs covers almost everything with one exception in hand and that is the consideration of consequences. Hence, the third major ethical approach is the Consequence-Based ethical view which is also known as Consequentialism. This approach postulates that the morality of any act can only be judged by the kind of consequences produced by that certain act. More precisely, this school of thought believes that any act is good only if it promotes more beneficial outcomes for maximum possible number of individuals than any other alternative of that respective act. This theory is usually associated with a famous proverb i.e. "*Greatest Good for the Greatest Number*". The traces of this view are believed to be much older than 18th Century, yet the formal presentation of this view can be seen in the work of Jeremy Bentham (1748-1832) and then John Stuart Mill (1806-1873). Both named it as Utilitarianism because they came up with the idea of quantifying pain and pleasure generates by any respective action consequently introducing the term “utility” which gave birth to the term Utilitarianism. Utilitarianism can be best understood by the following example i.e. There is a train cabin coming on a rail track and that track further sub-divides in two tracks. One track has five workers working on it while the other one has one worker. And the train must go on one of the two respective tracks but according to its defined route, it directs towards the track having five workers. And there is a guard watching this situation being miles apart, so if he flips the switch of the train to the track where it kills only one worker, then the act would be declared as moral according to Utilitarianism because the death of one worker is better than the death of fiver workers. If the guard would not do anything, then five workers would be dead consequently generating more pain and less pleasure making this act as immoral or unethical.

There are many other minor ethical theories also available but these three school of thoughts explained above encompass major part of the human tendencies towards morals. The core idea behind explaining these major ethical views is not to compare them with each other and to discover the authenticity of one of them consequently declaring it as the most plausible and logical ethical theory ever. Instead, the idea is to choose the most appropriate ethical theory that could best fit to our situation under consideration which is mass surveillance and Snowden’s Revelations in our case. Moreover, the reason behind discussing all the three major ethical school of thoughts is to back up our selection process with solid, rational, and logical reasons.

Brief introduction of the three major school of thoughts mentioned above exonerates us from confusion and simplifies our process of choice by presenting us a way to classify each of those views with an individual yet generalized trait as shown in Figure 10 below [75, Fig. 1].

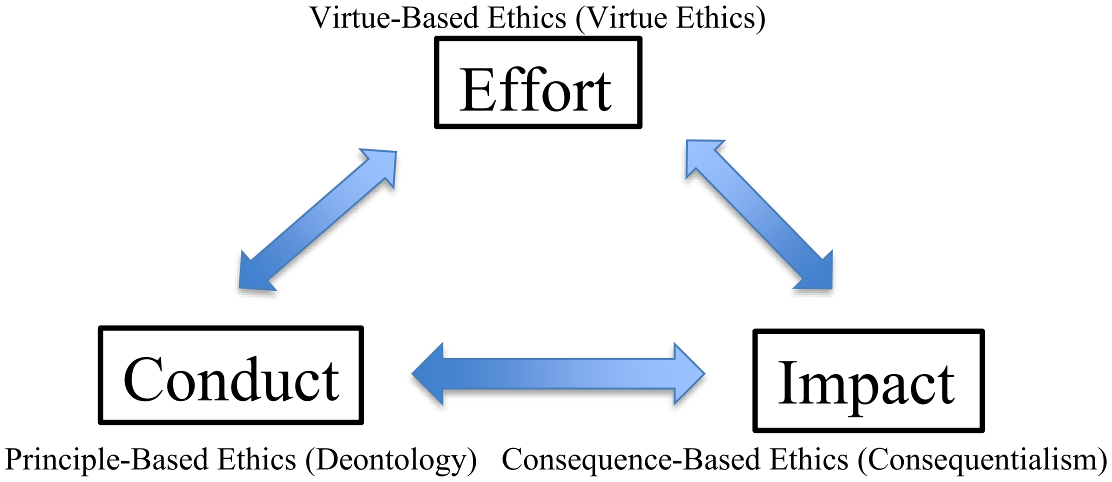

Virtue-Based Ethics (Virtue Ethics)
Effort
Conduct
Impact
Principle-Based Ethics (Deontology)
Consequence-Based Ethics (Consequentialism)

Figure 10: Three Major Ethical Views

Figure 10 represents a very important yet contradicting fact. All the three major ethical theories endorse each other’s views under certain conditions when needed by keeping their core concept intact. And this connection provides us with the facility of using multiple ethical theories on minor scale if needed to weigh any situation from multiple dimensions or to achieve the ethical approval of any act by multiple ethical views. It is because, all these three school of thoughts are further sub-divided in many minor views which intersects with each other at certain points on a micro level while the macro level and the core concept of all these three schools remains distinguishingly intact and unique from each other. So that is how, all these implications influence each other somehow, somewhere under certain situations. Moreover, Figure 10 significantly simplifies our thought process in choosing an appropriate ethical theory that could best fit to our situation. So, in this regard, we can see that Virtue-ethics represents "Effort" while Deontology represents "Conduct" and Consequentialism represents "Impact". And "Impact" is exactly what we intend to analyze through ethical lens in this thesis. Because, mass surveillance and Snowden's revelations are not about filtering anyone's efforts or conduct in order to declare these acts as ethical or unethical instead both are primarily concerned about the consequences that are being generated in result of both acts and it compels us to focus upon the utility produced out of them. Hence, we can conclude our choice by selecting Consequentialism/Utilitarianism as our base theory for analyzing our area of interest under consideration.

5.3 Utilitarianism

Despite the fact that Jeremy Bentham is being considered as the first one to release detailed research on Utilitarianism but still, history affiliates the Utilitarianism with David Hume[18] as the first person regarding the inception of concept of Utilitarianism although not formally but informally. Later, Jeremey Bentham in 1789 wrote his book explaining the details of Utilitarianism along with applications especially with respect to criminal and penal law. Later on, Stuart Mill[19], Henry Sidwick[20], R.M Hare[21] and Peter Singer[22] are some of the important names in the list of pioneers who contributed massively towards Bentham's work of Utilitarianism by making more and more rigorous and detailed researches in view of different aspects of human life consequently

[18] David Hume was a Scottish Enlightenment Philosopher, historian, economist, and essayist. He was born in the second decade of 17th Century in Edinburgh, Scotland. https://plato.stanford.edu/entries/hume/

[19] John Stuart Mill was a British Philosopher, civil servant and Political Economist. He was born in the start of 18th Century in London, England. He was an ardent advocate of Utilitarianism. https://plato.stanford.edu/entries/mill/

[20] Henry Sidgwick is being considered as one of the most influential ethical philosophers of Victorian era. He was born in 1838 in Yorkshire, England. He presented the culmination of work of John Stuart Mill and Jeremy Bentham regarding Classical Utilitarianism. https://plato.stanford.edu/entries/sidgwick/

[21] His full name is Richard Mervyn Hare. He was British Moral philosopher. He is famous for his work on the development of prescriptivism plus his preferences about the justification of Utilitarianism. He was born in 1919 in Somerset, England. https://plato.stanford.edu/entries/hare/

[22] Peter Singer is an Australian Moral Philosopher. His specialization is in Applied ethics and he supports morality from secular and Utilitarian perspective. He was born in 1946 in Melbourne, Australia.

applying and justifying the Utilitarianism through them. Among all of them, Mill's work has been the most widely read account on Utilitarianism. [65]

Utilitarianism can be defined as the system of thought that states that the best action in any situation is the one that brings most advantages to the most people [66]. Similarly, Encyclopedia Britannica describes Utilitarianism as a theory of normative ethics according to which an action is right if it promotes/produces happiness and its wrong if it produces the reverse of happiness [67]. There are many such ways in which Utilitarianism can be defined but all such definitions imply one prominent fact and that is "Utility". So, basically, Utilitarianism is based on the sum of total utility produced because of any action, and that is how the morality of that action could be decided as moral or immoral. There are two main branches of Utilitarianism which are,

- **Act Utilitarianism:** According to this theory, it promotes a mindset of performing any action which promotes maximum benefits for the majority without considering any personal feelings, societal aspect or even law. [68]

- **Rule Utilitarianism:** This branch considers law and promotes the mindset of creating maximum benefits or happiness for the majority by using most fair and just means available. This branch basically promotes justice and fairness. [68]

5.3.1 Views of Utilitarianism

The list of views related to Utilitarianism is quite long, but there are five major views of Utilitarianism which are widely accepted, discussed, and applied. So below are those five Utilitarian views on which Utilitarianism relies primarily [65],

- **Consequentialism**
- **Welfarism**
- **Individualism**
- **Aggregation**
- **Maximization**

5.3.1.1 Consequentialism

This attribute states that the morality of any act can only be judged by its end results or in other words, it can be stated that wrongness or rightness of any act is solely dependent upon what kind of consequences any certain act generates. In this way, any act can be considered as right if and only if the results it generates are as good as any other act that could have been performed instead it.

5.3.1.2 Welfarism

The idea of judging the morality of any act by the well-being or welfare it yields is described as Welfarism. But the idea of welfare or well-being is sometimes confused with happiness, while the welfare here does not mean anyone's mental state for the time being at any instant instead it implies the general flourishing of an individual or a community. Hence, any certain act is better than the other if an only if it results greater amount of wellbeing or welfare.

5.3.1.3 Individualism

This thinking is based on the idea that only the individuals are the entities that are supposed to be considered as objects of moral regards but not the nations, tribes, groups, or communities. Hence, it applies that only the individuals e.g. person or animals are the sources of values in terms of considering moral regards.

5.3.1.4 Aggregation

This view can be considered as another dimension of Individualism, but this view states that the worth of any kind of act or states of affairs can be determined by summing up the value produced by or associated with all the individuals involved or attached to that respective state of affairs. So this view also somehow focusses on individual worth of entities involved in any act but it believes on considering a joint outcome by taking into account the summation of every single output attached or produced by every single individual involved in that certain act.

5.3.1.5 Maximization

This view supports the outcome or worth of any act or situation to be as great as possible. In order to understand this view, we can suppose that if there are two groups of people in such a way i.e. the first group of people is not very well-off but they are numerous in their number and the value produced by every individual of this group would be greater than the other group in which majority individuals are very well-off but that group has lesser number of individuals and the value produced by these individuals would be less than the first group. So, in this way according to the maximization view of Utilitarianism, the act associated to the first group must be preferred over the act associated with the second group. Among all the five views, this view has least number of controversies and contradicting views.

5.4 Utilitarian Analysis of Mass Surveillance Enroute Snowden's Revelations

Ethics in mass surveillance and human rights are inextricably connected due to which there is a very thin border line between both, and it could be crossed even with a very slight deviation. But the point is that which specific human right could be influenced by surveillance and needs to be discussed in the light of ethics? That human right is "Privacy". Privacy is the fundamental right of every human being and it has been stated in many legislations across the globe e.g. The Universal Declaration of Human Rights (Article 12); The International Covenant on Civil and Political Rights (Article 17); The European Convention of Human Rights (ECHR) (Article 8); The Charter of Fundamental Rights of the European Union (Article 7) and the American Convention on Human Rights (Article 11) and out of all these international legislations and agreements, Article 8 of ECHR has been more widely accepted [69, p. 36] and along with declaring Privacy as a basic human right, it also clearly defines the boundaries under which the privacy of any individual could be infringed by government authorities but the question about the mass surveillance established by individuals or private organizations still needs to be addressed in terms of Ethics because although, the privacy of individuals has been unequivocally accepted as a basic human right, yet we see the ethical as well as legal violations in this regard which consequently imbalances the overall mindset of the social infrastructure.

Although the actual awareness drive primarily started on international level right after the Snowden's revelations, which consequently made Edward Snowden as a legendary as well as a public figure globally because of apparently unveiling the most insidious secrets of intelligence community, yet there are some other sides of this picture which are unseen and unheard. Snowden's revelations and the consequent stir those revelations caused represents merely one side of the picture due to which ethical implications or frameworks are not justified enough to be applied bluntly instead the picture must be viewed from all possible angles so that a broader as well as all the hidden dimensions of this situation could be explored before jumping into conclusions directly. Because Snowden's revelations influenced three most important elements in terms of ethics not just among masses but among nations as well i.e. Trust, Dignity and Privacy [69, p. 66]. Snowden's revelations exposed majority of the minor or major surveillance operations ever executed by USA's intelligence community directly or indirectly at any scale which consequently exposed not just the masses being monitored but few head of the states as well which included some from EU as well consequently this exposure was viewed as a serious ethical crisis both on individual scale as well as internationally followed by serious political repercussions. Moreover, it influenced the social fabric among masses and somehow international political alliances as well [69, p. 67].

Globally, Snowden rapidly gained the title of a whistleblower or savior while according to the US law as well as the review made by the US house of representatives, Snowden committed a treason and this accusation makes the situation difficult to be analyzed from ethical point of view without questioning the Snowden's loyalty with his job description, with his organization and his country as well [70] so, he must pass both the Rule and Act Utilitarianism test in order to get entitled as a Whistleblower ethically. Hence, in the light of the review presented by US house of representatives on the actions of Snowden, out of whole document, three major accusations posed against Snowden are as follows,

1- Snowden is responsible for causing damage to national integrity and security because the documents he revealed had nothing to do with the surveillance of masses on individual scale, that's why none of those programs were affecting individual privacy concerns instead all those programs were related to Military, Intelligence, and defense against American adversaries so leaking out such programs gives the enemies a competitive advantage. [70, p. i]
2- Snowden cannot be considered as a whistleblower because under the American legislation, anyone revealing classified information publicly does not qualify him/her as a whistleblower. However, disclosing any kind of classified information regarding abuse, fraud, or any illegal activity to the relevant law enforcement authorities or to the seniors does qualify someone as a whistleblower. Moreover, contrary to his claim that Snowden tried informing higher relevant authorities in this regard, there exists no such evidence. [70, p. ii]
3- In contradiction to the public claim made by Snowden that he was afraid of facing some sort of retaliation, there is a law available for it which shelters him

> with immediate protection. And the committee regularly receives disclosures from all such whistleblowers who are being protected under the Intelligence Community Whistleblower Protection Act 1998 (IC WPA). [70, p. ii]

Before moving on any further towards Utilitarian Analysis, one thing needs to be clearly understood that why throughout the discussion in this thesis, only USA remained in limelight so far? There is one very solid reason attached to this question i.e. USA has a very significant importance in terms of global privacy issues not only because of its global weight, nuclear/armed dominance etc. but because of its undoubtedly enormous ownership in terms of companies providing internet services across the globe. And secondly the Snowden's revelations added more to its importance and brought USA under the global debate. Moreover, USA has a long history of formulating innovative legislations for privacy protection [69, p. 36].

There are apparently two bases available to weigh the Mass surveillance, Snowden's revelations and the accusations posed on Edward Snowden by US Government in ethical scale i.e. Utilitarian approach and the Ethical Analysis available in ECHR. So, in this regard, the core ethical principles recommended by EGE (European Group on Ethics) to ECHR are as follows [69, p. 71],

- Privacy & Freedom
- Autonomy & Responsibility
- Well-Being &/or Human Flourishing
- Justice

Moreover, EGE presented two more principles which must be adopted to maintain trust among governments as well as among individuals and governments/private organizations. Those two principles are as follows,

- Transparency
- Efficacy & proportionality

These principles were presented to maintain a balance among security and privacy and the principles which could define a barrier in terms of ethics. These principles also imply Utilitarian views as shown in Figure 11.

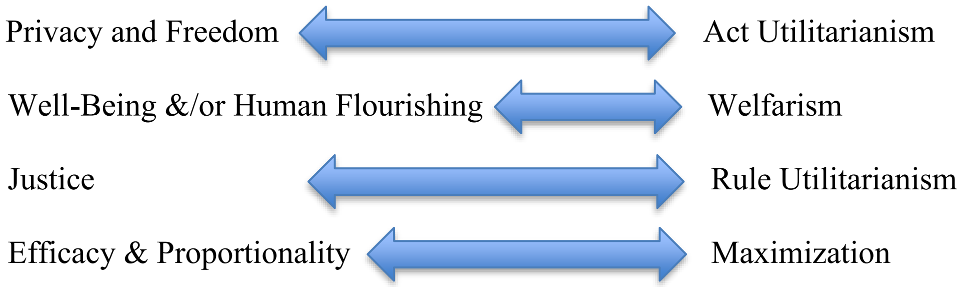


Figure 11: EGE Implying Utilitarianism

Figure 11 clearly justifies the choice of using Utilitarianism as a base ethical theory to justify the ethical analysis of all the factors discussed in this thesis.

Now we will analyze all the three major accusations posed on Snowden by US house of representatives sequentially from ethical point of view. As per first accusation mentioned above, it is being declared that Snowden caused damage to national security because none of the programs belongs to any act which could hit individual's privacy concerns. To analyze all the possible dimensions of this accusation, we need to refer to Section 4.3.1.1. This section is about both types of surveillance that were revealed in the leaked documents i.e. Upstream and downstream surveillance. So, PRISM was the part of downstream surveillance in which nine major internet companies of USA were providing data of individuals to USA's intelligence community without being consensual with those respective individuals. Moreover, USA's intelligence community initiated operation Upstream which had multiple sub-operations e.g. BLARNEY, OAKSTAR, FAIRVIEW etc. and Upstream was primarily about tapping underwater optical fiber cables of internet in order to monitor every single piece of information of every single individual whose data is traveling through those cables. Hence, all the proves given through leaked documents contradicts as well as undermines the claim made in the review by US house of representatives against Snowden in this first accusation. Snowden's revelations damaged the national security or not, but yes! all those revelations really damaged the national integrity which was inevitable. It damaged the trust level between government and masses. Moreover, it shook the trust of USA with its alliances especially from European Union [69, p. 66]. Hence, there comes four views in support of Snowden from ethical point of view i.e. Act Utilitarianism, Consequentialism, Maximization & Individualism. Snowden did what he felt was right without considering how it would affect himself or to his personal feelings/emotions because he preferred the utility of his act more than the consequences he would be facing afterwards. Secondly, he knew the consequences already that it would cause a sense of mass awareness consequently urging international authorities to take relevant measures accordingly, so that is why he did not hesitate to make the revelations. Thirdly, he focused on the value that would be created by majority of the people who are not well-off i.e. every single average internet user, rather than the value created by few well-off people i.e. USA's intelligence community. Lastly, he endorsed Individualism through his act by flaming awareness about illegal privacy infringements of individuals not merely within USA but in different parts of the world. He preferred the privacy rights of every single individual instead of preferring the stakes of intelligence community which directly implies Individualism. So, based on all these proves, Snowden's act of revelations illuminates itself as justified as well as ethical and furthermore it rejects the first accusation made on Snowden by US house of representatives in their review because contrary to what the revealed documents exposed, this first accusation appears to be merely forged. Hence, in case of the first accusation, Snowden Passes the Act Utilitarian test but not Rule Utilitarian test because this accusation is solely about the consequences generated out of his act but not about the way through which Snowden committed the act.

Moving on to the second accusation, that according to the US law, Snowden doesn't fulfill the parameters to hold the title of a whistleblower because revealing any classified information publicly doesn't make someone as a whistleblower as per US legislations of Intelligence community. So, the analysis of this situation in the light of Utilitarianism appears to be perplexed because this accusation can be backed by one or two views of Utilitarianism while it can be opposed by some of them as well. So according to the "Rule Utilitarianism", Snowden's act of revealing classified documents cannot be entitled as ethical or moral because apparently, he contradicted the law of the land and he did not use the most just means available. He would pass the Rule Utilitarian test only if there are evidences available that he tried to reach his superiors before making the revelations public. It clearly states that, he didn't use the most just means available because in this accusation, it's been mentioned that making any such revelations regarding any unlawful activity within intelligence premises only to the relevant seniors or law enforcement authorities entitles someone as a whistleblower, consequently which makes this act of Snowden as completely immoral and unethical according to Rule Utilitarianism. While according to the Consequentialism and Welfarism, we can entitle Snowden's act as somewhat moral or ethical. Because there are two kinds of consequences produced by his act i.e. Individual and global. For him as an individual, the consequences didn't prove situation friendly towards him at all instead it ruined his career as an intelligence agency contractor in NSA, it disturbed his family life and prohibited his life-time entrance in his own mother-land consequently tagging him as a threat and a traitor on national level. But on the other hand, the consequences of his act stirred a sense of global awareness among masses at all scales e.g. economies, governments, organizations, entrepreneurs, intelligence community etc. So, in short, he sacrificed his individual motives in order to generate more utility for the majority by raising voice against un-consensual and hidden mass surveillance which urged the authorities globally to reform their legislations which again implies that he passes Act Utilitarian test. But Utilitarian thinking never considers the consequences that the individual who performs the act might have to experiences. So, the utility generated by the consequences of his act of revelation declare his act as an ethical as it implies Welfarism as well as Maximization. Hence, this second accusation by US house of representatives appears to be unethical from one dimension according to one view of Utilitarianism, while two views appears in favor of this act as moral so through consensus, we can call his act as moral because more views appears in its favor but still the unethical aspect of this act cannot be forsaken as it implies a treason consequently making this unethical aspect as of an enormous significance. Because Mill states that some pleasures generate more utility than others, similarly some pains produce more unhappiness than others. Hence, in case of this second accusation, both Act and Rule Utilitarian tests applied on Snowden's act and he passes the former while fails the later one consequently making his act more inclined toward immorality.

The third accusation again somewhat appears to be giving a diffused outcome in terms of declaring Snowden's act as ethical. Because it also implies the law which Snowden was supposed to abide by but unfortunately, he did not do so which consequently makes him more of a criminal and less of a whistleblower. The third accusation points out the law which protects the personnel who wants to make any kind of revelations about intelligence community to the relevant law enforcement authorities. But Snowden being afraid of retaliation instead of protection, didn't go for the legal protections because he wasn't sure if being a contractor he is also eligible for the protection under the Intelligence Community Whistleblower Protection Act 1998 (IC WPA) or not [70, p. ii]. So, that is why being afraid he made the revelations publicly by leaking out classified documents of USA's intelligence community. But the law confirms that Snowden even being a contractor was also entitled for the legal protection under IC WPA without facing any kind of retaliation from the law enforcement authorities. So far, the Snowden's act appears to be unethical in the light of Rule Utilitarianism because he did not utilize the most just means available. But there is one most important point which endorses the shaken confidence of Snowden over law enforcement authorities is as follows,

"(U) Snowden, however, has argued that even a lawful disclosure would have resulted in retaliation against him.
(u) Among other things, Snowden has argued that he was unable to raise concerns about NSA programs because he was not entitled to protection as an IC whistle-blower given his status as a contractor. (He was with Booz Allen at the time of his leaks to the press.) But the 1998 IC WPA applies to IC employees as well as contractors. Although the statute does not explicitly prohibit reprisals, the IC WPA channel nevertheless enables confidential, classified disclosures and oversight, as well as a measure of informal source protection by Congress. The statute specifically authorizes IC contractors to inform the intelligence committees of adverse actions taken as a consequence of IC WPA-covered disclosures." [70, p. 18]

So this clause of the review presented by US house of representatives about Snowden's revelations clearly states two important yet contradicting facts, i.e. Snowden even being a contractor was entitled to legal protection if he had made the revelations to the relevant authorities and secondly, that there is no explicit clause in IC WPA which prohibits reprisals. So, now we can clearly understand that why Snowden was reluctant to express his concerns with the seniors of NSA and why he was more inclined and convinced to make the revelations publicly and what was the reason behind his shaken confidence over the NSA's authorities? Although there exists a law which declares someone as a whistleblower and protects him/her later, but that same law lacks the confidence of not having a retaliation against any such personnel specifically and formally. Hence, once again the ball is in the court of Snowden from ethical point of view. Although there was a law, but the law was not competent enough to address all the possible concerns of Snowden or any such personnel which consequently compelled him to use the other way. The same law which acts like giving protection to the whistleblower also kept an open window for having retaliation against such personnel which consequently doesn't make the law even ethical enough to cater the concerns being trust worthy enough, so no wonder, why Snowden took such a bold step by disturbing his whole life style consequently ended up in an asylum in Russia. Moreover, the law also ignores Individualism. Hence, in this case, along with giving generally a conflicting outcome, this accusation also ignores Individualism which endorses Snowden's act as ethical because he specifically addressed Individualism which makes him qualify Act Utilitarian test.

There is a list of many other accusations as well posed by same authorities, which may or may not be proved ethically or morally right but weighing the major three accusations in ethical scale affirms about Snowden has been rightly tagged as a Whistleblower. And at the same time, it renders the debate about declaring mass surveillance as ethical or unethical.

Hence, as per the above discussion, Snowden does qualify as a Whistleblower from Utilitarian point of view because of the outcomes generated by his act and the ethical contradictions found in the three major objections posed on him by US house of representatives. In order to have a better analysis of mass surveillance in the light of Utilitarianism, we will now segregate the parties involved in this situation in order to measure the consequences created by each one of them respectively and then we will measure the overall utility of the situation. There are three parties involved in this act, Edward Snowden, Surveilling authorities (State and non-State Actors) and masses. But for the time being we will consider only state surveillance apparatus while neglecting the non-state actors involved in it because the idea is to analyze mass surveillance ethically in general but not to measure the utility associated with surveillance activities of every actor involved in it separately. Moreover, the awareness drive primarily highlighted government as the backbone infrastructure behind surveillance in general. That is why it is deemed important to analyze state surveillance apparatus ethically to have a general understanding of mass surveillance from ethical point of view.

There are many theories available which could weigh the morality of state surveillance apparatus but the choice of Utilitarianism here is because it primarily focusses on the outcome as well as the quantum of utility or happiness created for maximum possible number of people. First, the motive of US government behind establishing such an organized state surveillance apparatus needs to be considered which is the security of US citizens from any internal or external threat or terrorism in general. But the question comes up here that what should be the way for any government to establish such surveillance activities so that such measures does not contradicts with basic human rights and morals/ethics? Moreover, Utilitarianism does not consider intentions behind acts at all instead it solely relies on the outcomes generated regarding the quantum of their utility. Hence, we are compelled to unpin the intentions of US government or any government in case they try to justify state sponsored surveillance with an intention of security of citizens. The security of masses in also one of the basic human necessity but again it hasn't been made clear by US government after being exposed that what is the best ethical way to provide security to masses without infringing their basic human rights? While Privacy holds the primary importance in this regard. So instead of devising an ethical way for surveillance, the government tried to defend all of their operations by accusing Edward Snowden of treason and by elaborating their intentions behind all kind of surveillance activities and by using some other forged statements in this regard as well as seen above in the accusations posed on Snowden.

Undeniably, it is agreed that state's safety is a top priority and the only way to achieve state's security is to pre-analyze and rectify the threats before any calamity occurs. It is only because, prevention is always better than cure and using reprisals later are not productive enough the way they could be if done before hand to prevent any act of terrorism or violence. And American Government defended their stance regarding mass surveillance in the name of state's security which eventually means securing citizens/masses. Utilitarian philosophy also endorses this view consequently supporting pre-emptive measures of prevention rather than relying on retaliation. Because, according to Utilitarian thinking, such precautions will result as a peaceful living situation for masses which clearly shows that Utilitarian thinking does not support the justifications based on intentions of US government instead it supports the outcomes that could possibly be achieved in result of mass surveillance even though it's been not made clear that what is the effective and ethical way to achieve state's security? Because Utilitarian thinking views American public in general as an entity which would get the consequential benefits of having peace irrespective of the way adopted to execute these safety measures. And that's how NSA's mass surveillance activity would qualify for "Act Utilitarian" test due to its safety measures prevailed for maximum number of people which tag this safety as a good to be done for masses. Hence, by looking at the justified outcomes that could generate maximum security which can be translated into maximum good for maximum number of people residing within national boundaries consequently endorses that Utilitarian thinking supports the state surveillance apparatus and affirms it as ethical in general but only through the lens of "Act Utilitarianism". "Rule Utilitarianism" would be more appropriate approach to be used in order to measure the negative outcomes of NSA's mass surveillance activities that impacted people in the longer-run because of using deceptive means to provide safety to people by violating a generally accepted moral and legal value.

Initially there was a denial from government officials as well as from the intelligence community about any such organized mass surveillance as revealed by Snowden's leaked documents. But later, after realizing the intensity of the public outrage and media reporting, finally the government officials not just confessed instead defended those mass surveillance activities as well. Out of many officials, two names are important to be mentioned here to represent the governments narrative regarding the situation: First, the Senator of California Dianne Feinstein and second the Director of NSA, General Keith Alexander. Dianne Feinstein made a public remark by quoting a famous MacCarthic[23] quote that "*There is no harm in collecting information because if you are not guilty, you have nothing to fear"* [77, p. 608]. Similarly, in another instant the director of NSA Keith Alexander defended operation PRISM (refer to chapter 4) that "*It operated with full oversight and that is a lawful intercept program for foreign intelligence. We have a metadata program that helps us to connect the dots in least intrusive way"* [78]. In short, ultimately government officials and intelligence community confessed all the accusations revealed in leaked documents by Snowden as truthful and real, consequently played a tactic to slowly poisoning the masses to make them comfortable about mass surveillance as a new normal and it is for the greater good of everyone consequently generating more utility in the name of state's security as a collective outcome. Furthermore, NSA and GCHQ (General Communication Head Quarters)[24] both defended state surveillance apparatus by claiming that pervasiveness and secrecy both are compulsory to run such programs otherwise the world would go dark. So, according to the claims of both these organizations, the insidious operational mode of state sponsored surveillance helps the good guys to keep tracking the bad ones consequently preventing another calamity like 9/11 and that's the only way to keep the world "go light". They added further to their claim that our activities should not be regulated and the amount of data we can collect must not be limited because if it happens then we might go blind to track the bad guys [79].

[23] MacCarthic quote means to present an accusation/argument without having any regard of the evidences.

[24] It's an intelligence agency of United Kingdom, whose core function is to provide signal intelligence (SIGINT) to the British Government and Armed Forces. https://www.gchq.gov.uk/

The terms “Go dark” implies being blind of the suspected threats and “Go light” implies being aware of the suspected threats.

All the claims stated in the above paragraph apparently presents very illuminating consequences in terms of creating utility for masses in the name of state’s security consequently declaring state sponsored surveillance as an ethical activity. But all this debate still renders one problem because all such claims referred to as public security ignores morality & individualism entirely and all such claims must also pass the “Rule Utilitarian” test to achieve an ethical status. So, all such claims, confessions and justifications given by government officials and intelligence community in defiance of the accusations posed by leaked documents, the intention of mass surveillance clearly reflects the attitude of treating masses not as individuals but as a community in general consequently negating the utility of individualistic approach of Utilitarian thinking entirely. It is because, ethics emphasizes on basic human rights of every individual by considering those individuals not merely as citizens but persons as well. In this case, the basic human right is privacy which has been guarded by Fourth Amendment[25] which endorses prevention of any kind of unreasonable scrutiny of any individual. So that’s how, state surveillance apparatus in case of NSA neither qualifies individualism criterion nor it passes “Rule Utilitarian” test because one thing has been clearly understood since the day Snowden revealed the documents that every single surveillance oriented operation of US government/Intelligence Community was insidious and American citizens were completely unaware of it which consequently states the fact that “most just means available” is not the part of any surveillance operation. Moreover, it also violates fourth Amendment. Therefore, it can be said that this state sponsored surveillance stripped both the moral as well as legal rights of American citizens. At this point, the ambience of this analysis implies an obvious conclusive outcome but still, there is another angle as well from which this situation must be analyzed before drawing any final conclusions and that is Snowden’s perspective.

Snowden executed his act of revealing classified information purely based on Utilitarian thinking because Utilitarianism does not consider whatever consequences would occur to the one performing the act. Similarly, on the other hand if he would remain silent, his act would be translated as egoistic which implies another consequentialist approach known as ethical egoism according to which any act is moral if it generates more happiness for the decision maker than it generates for the others [80, section. 2], [81]. Having ethical egoism doesn’t makes the act of an agent as unethical, instead it contradicts with the core philosophy of Kantianism and Utilitarianism as both of them states that one must prefer interest of others over self-interest consequently giving more weight to the interests of others which also implies Mill’s proposition that some pleasures carries more weight than others [80, section. 2], [97, section. 2.2]. Therefore,

[25] It is the clause of Bill of Rights in United State’s Constitution. According to this clause, any unreasonable search and seizure of any individual is prohibited. Moreover, it sets the mandatory requirements for issuing warrants against any individual: Warrants can only be issued by judge or magistrate followed by a justified cause behind any search endorsed by an Oath and affirmation and it must also include the details of the place, thing or a person to be searched.
https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0

being silent, Snowden's act would have failed the test of "Act Utilitarian" because it would have caused the reverse of happiness by keeping millions of people being unaware from having their moral and legal rights being stripped away by state sponsored surveillance apparatus in the name of security which also implies his egoism as well. But instead of choosing silence, he chosen whistleblowing by ignoring the consequences for himself and generated utility through awareness by unveiling an unlawful operational activities because he was more concerned about the innocent people that were exposed to unlawful scrutiny, criminalization and monitoring at the cost of their legal and moral rights. He sacrificed his own comfort/happiness for creating maximum happiness for others because now Americans are not ignorant anymore instead, they are fighting to secure their moral right of privacy which is being endorsed legally as well in Fourth Amendment. So, that is how his act passes both the "Act" and "Rule" Utilitarian tests. While state sponsored surveillance passes Act Utilitarian test but does not qualify Individualism as well as Rule Utilitarian test because of using insidious and not the most just means available while both these approaches must be a mandatory part of any organization's legitimate code of ethics.

In another analysis, lets segregate the positive and negatives consequences and measures them separately in the light of Utilitarianism. There are three parties involved in this scenario as stated above i.e. Public/masses, Government/Intelligence and Edward Snowden. Snowden's act of revelation is the base reason behind all the consequences generated irrespective of their positivity and utility produced out of them. In Utilitarian terms, NSA and GCHQ defends surveillance by claiming that it generates happiness for everyone in the name of state's security, because if there is no security, there could be attacks anytime consequently every citizen would be in lifetime danger which implies that if there is no life security then every other pleasure is useless. While, on the other hand, such intelligence programs cause unhappiness for the citizens because of stripping down their moral and legal right by invading their privacy via nonconsensual and unlawful means. That is why there needs to be a maximization of happiness for everyone that is involved in the scenario under consideration according to Utilitarian thinking. So, intelligence community defends this point by claiming the fact that not every happiness bears equal weight instead some forms of happiness bears more weight/importance than others by referring Mill's point of view [97, section. 2.2]. Because Mill believes that not all pleasures are same. Some pleasures bear more ethical value than others. That is why, the pleasure generating more happiness/utility must be preferred over the other. So, as per the claim the of NSA and GCHQ, we can assume that they allocate more moral utility to security than to privacy/freedom of masses. Means, if there is no security, there is no privacy and freedom because attackers/terrorists could strip both these rights anyway anytime. In short, inverse analysis of NSA & GCHQ's claim implies that the pain caused by terrorists would be greater than the pain or unhappiness caused by intelligence community by stripping rights of freedom and privacy un-consensually. Mill also claims security as a form of pleasure that is qualitatively superior in terms of utility than any other competing pleasures [82]. Hence. NSA & GCHQ's claim really seems justified based on Mill's endorsement about security as an indispensable pleasure.

But the concept of measuring pain and pleasure presented by Mill states that either one of them can be preferred on the other one only by the individual who is actually going through either one of them and who actually experiences the situation and who is intimately familiar with the intensity and presence or absence of both pain or pleasure [83]. But the instances reported by journalists and many other forums states that most of the high officials overseeing the intelligence community doesn't even understand the internet completely consequently they are unaware of the capabilities of the system deployed by intelligence community and its far-reaching consequences [79]. Hence, NSA and GCHQ lose the right to justify the superiority of any pain or pleasure involved in this scenario. Because the personnel who designed, deployed, and monitored the entire complex infrastructure for surveillance never made any public appearance while the one making public appearances has poor technical understanding. That is why NSA & GCHQ's high officials cannot quote Mill's criteria of measuring utility of the pain or pleasure involved in this process. Hence, public lefts out as an only entity who might be a victim of nonconsensual and unlawful state sponsored surveillance or the attacks of terrorists. So, the decision responsibility in this regard shifts entirely upon the masses to decide which pleasure is better and what is the suitable way to fulfill that certain pleasure and through which acts that respective pleasure could be achieved in a way that it causes maximum happiness and minimum pain? Public outrage after Snowden's revelations helps us to resolve this discussion in terms of choosing the kind of pleasure public wants to have is privacy and freedom over security or unlawful mass surveillance.

Moving towards conclusions, there are certain factors which have been aroused out of this analysis according to which, masses aren't much concerned about the mass surveillance, instead they were more concerned about the ways which are in practice for executing surveillance tendencies along with many other allied factors. So, this scenario poses some questions for authorities having surveillance tendencies which are as follows,

1- Are the higher officials overseeing intelligence community fully understands the capabilities of the deployed state surveillance apparatus?
2- Have the individuals under surveillance given their consent about data collection of their personal information?
3- Are the consented individuals informed about the extent of surveillance being deployed on them?
4- Does this surveillance cause any psychological or physical harm to anybody publicly or privately?
5- Are the individuals aware about the identity and intentions of the surveilling authority?
6- What kind of techniques are involved in surveillance and are the individuals under surveillance aware of them?
7- What are the expected findings out of the data collection and are the individuals being surveilled aware of them?
8- Does the methodology applied for surveillance adhere both the legal and moral/ethical rights of masses under surveillance?

Hence, all these questions provides us with a rough form of a framework which can be refined with more research about the concerns that must be addressed before deploying any kind of mass surveillance apparatus whether government or private in order to get it done legally and ethically. The conclusion of this analysis can be applied in any social setting if, as a society we truly seek morality in terms of surveillance activities.

Chapter 6: Legal & Cultral Implications

Societies have always been an amalgam of legality and morality. Legality is implemented via judicial infrastructure of any country which is primarily a subset of national constitution. While morality on the other hand is mostly not a documented framework, but still, it has been deeply rooted even more than legality among the individuals of any society because it is a direct product of cultural values. And culture is always a derivative of certain social practices that have been flourishing in any society since centuries. Although over the time, culture experiences certain variations, yet its core structure remains intact. Moreover, legality always gets enforced over masses while culture is a built-in trait of any social setup which consequently plays major part in shaping ethical framework of any society.

This chapter addresses the ethical implications in terms of laws and culture. It presents a generalized analysis of how ethics are influenced by law and culture and vice versa in any social setup.

6.1 Legality

Espionage, spying, or surveillance activities are commonly occurring phenomenon in the war-time situations or among nations having conflicting international stances. But now even in peacetimes, mass surveillance has become an activity which is happening around the clock 24/7 and this is what stirs the masses especially after Snowden's revelations. So the usual reply we get to hear from surveilling authorities is that it's being done in order to prevent any kind of expected danger or civil-war or protests or any kind of other distressed situation going on within borders or any kind of expected attack from foreign as well as domestic actors as explained in above chapters. But the surveilling methodologies and its consequences shows the results otherwise, it shows few other dimensions as well in parallel with the ones stated by authorities in above chapters. Actors involved in surveillance activities are usually linked or become linked under certain circumstances when needed and every actor has his/her own personal stake as explained above in section 4.3.1 and 4.5. In the case of government agencies maintaining mass surveillance, stakes could be national integrity but in case of individuals or private technology giants, stakes involves data collection, its sale and purchase, synched advertisements, attribute profiling and so on and so forth. Therefore, there is a dire need to consult are there any laws available that cater this situation from ethical point of view? If yes, then how?

An overview of some of the global legislations which plays the role in guarding the privacy or curbing the scope of mass surveillance introduces us with following documented practices which implies ethical concerns [69, p. 36],

- Tort Breach of Confidence.
- Human Rights Act 1998.
- Data Protection Act 1998.
- Regulation of Investigatory Powers Act 2000 [71, pp. 65-71].
- The Universal Declaration of Human Rights (Article 12).

- The international Covenant on Civil & Political Rights (Article 17).
- The European Convention of Human Rights (Article 8).
- The Charter of Fundamental Rights of the European Union (Article 7).
- The American Convention on Human Rights (Article 11).
- Right to Freedom of Expression of European Convention of Human Rights (Article 10).
- GDPR (General Data Protection Regulation): Article 16, 22, 55 etc. [87].

The global overview of listing down the available legislations which could bolster the sustenance of the privacy of individuals provides us with many internationally accepted laws available but despite this fact, we have experienced severe violations in past with no accountability charges over the actors behind those violations which compels us to believe that either the laws are not competent enough to carry the balance between security and privacy of individuals, nations and organizations or there is no actual implementation of any of these laws from ethical point of view. The idea is not to compare all the international legislations in terms of ethics and finalize the best one instead the motive of listing down the international legislations above is to know that are there even any laws other than ECHR that guards the privacy rights of individuals. So, the above list clearly implies that many laws other than ECHR are there which presents with documented legislations regarding privacy.

6.1.1 GDPR (General Data Protection Regulation)

It has been applied in its full form in 2018 and it was primarily formulated to harmonize the data protection regulations and privacy concerns within Europe. Analyzing the privacy-oriented legislations from ethical viewpoint is a perplexed activity because social fabric within any region across the globe usually works in terms of what is legal instead of what is ethical. But yes, it is surely a plus if all the laws envisage ethical implications as their base consideration behind formulating any law in parallel with legality. Similarly, GDPR does not specifically discusses ethical aspects instead it implies the factors that coincides with ethics and morals consequently presenting itself as a documented guardian of privacy oriented ethical rights along with legal ones.

The core structure of laws implies what must and what must not be done without regarding any ethical aspects while ethical definitions of good and bad lie behind such implications. Similarly, data protection rights also endorse privacy concerns as a fundamental right with the notion of considering them as an ethical aspect in general. Whatever has been accumulated in GDPR implies ethics in general being scattered in various chapters across the document consequently making their appearance as fragmented, blur and lacks explicit prominence. Although the ethical principles on which GDPR could have based are wider yet GDPR is a principle-based approach in parallel with being a rule-based approach.

6.1.1.1 Privacy Protection & Dignity

Charter of Fundamental rights of European Union declares dignity as one the base aspects of any human's life and stress upon it explicitly as follows in its article 1 [84] as follows,
"Human dignity is inviolable. It must be respected and protected."

Dignity has a very distinguishing position in ethical philosophies. Immanuel Kant[26] is among some of the most famous Deontologists (Refer to section 5.2) who declares dignity as an inherent worth of any human being. Kant further refine this concept by claiming that "*Human beings must not be treated merely as a mean but as an end*", in short, no human being must be considered merely as a source because this is what degrades his/her dignity [85], [86]. So, in this regard, Article 88 of GDPR presents very explicit guidelines by emphasizing that data protection oriented regulations, systems and infrastructures both technically as well as legally must be designed in such a way that they make sure the safety of human dignity and other fundamental rights consequently safe guarding the subject's data along with other basic human rights. Moreover, Article 5 also presents this concept from the point of Fairness and Transparency. The concept of fairness and transparency is very vast and variable due to which it is quite a cumbersome task to confine this concept under fixed set of rules. It is because, being a variable factor, it can be decided accordingly in relevance with the ethical and legal requirements of the scenario under consideration [87].

6.1.1.2 Rule of Law

Rule of law is another ethical as well as legal aspect that binds the masses, organizations, and countries to perform their duties by using most just means available which implies Rule Utilitarianism (Refer to 5.3). Article 6 of GDPR handles this situation quite clearly by stating that any kind of processing of personal data must include the consent of subject. This consensual processing of data has been addressed both in Article 6 and 8. Article 8 addresses the scenario where the subject is a child [87]. Along with consensual processing of data, Article 6 also presents conditions related to public interest consequently implying the concept of maximization not specifically but indirectly.

6.1.1.3 Surveillance

Surveillance isn't merely the monitoring of masses or individuals instead it invokes data collection, processing and data transfers from one authority to another by both government and private actors for fulfilling their various motives which may or may not hit the individuals in different ways both ethically as well as legally. In terms of ethics, there are three elements which must be considered before executing any surveillance activity which are as follows [88],

1- Means by which surveillance is being carried out and data is collected.
2- Are the individuals aware that their personal data is being collected and who collects it and why?
3- What are the goals of the surveilling authority behind this data collection?

Legal Implications: GDPR doesn't provides any concrete set of rules or laws which could balance the situation between privacy and security, because surveillance is a very vast concept which is always glued with the privacy and security concerns consequently demanding a balance between these two factors in order to make any surveillance activity as legal and ethical. GDPR addresses wide range of situations in general and yet it presents no formal statement setting up the rules which could declare any surveillance

[26] Immanuel Kant (1724-1804) is a German Philosopher who is famous for his work on Deontological aspects of ethical theories. https://www.iep.utm.edu/kantmeta/

activity as legal or illegal, ethical, or unethical. Article 5 (a) of GDPR addresses surveillance by leaving the surveillance activities at the discretion of national jurisdictions of the respective country which indirectly implies Rule Utilitarianism but at the disposal of law of the respective land because using the word Lawfully implies a vast scope without stating any specificity. But yes, Article 88 (3) highlights little more specific concerns in this regard by asking the member states to provide their jurisdictions in this regard [87] which gives us a hint of developing centralization among all the member states in terms of laws addressing various concerns related to information/data.

Authoritative Implications: Power relationship between surveilling authority and the subject presents a very important relationship because surveillant's power advantage may result in a personal harm to the surveilled. That is why, there is a need to address this concern because any imbalance in this situation and the consequences generated out of it implies serious ethical implications. Article 6 (1F) of GDPR handles this situation by stating the fact that, data can be processed only till the point of achieving legitimate interests of the surveillant except where such interests violates any fundamental human right of the subject [87]. Hence GDPR considers both legal as well as ethical aspects while addressing power relationship between the surveillant and the surveilled because privacy is among one of the fundamental human rights.

Scope: Surveillance can affect different individuals in different ways which primarily depends upon the following factors (refer to section 3.4). Therefore, in this regard, following concerns needs to be addressed to declare data collection as ethical and legal,

- The basis on which data is being collected?
- How the targets are being identified for surveillance? E.g. individuals, masses etc.
- Moreover, in which form, data is being collected and through which possible ways?

Deliberately targeting individuals, failure to measures the differential effects that could harm the dignity as well as privacy of individuals, unauthorized data distribution etc. and many such ethical issues needs to be addressed, but unfortunately GDPR doesn't cover any such aspects consequently posing a demand of upgradation in this legislation [87].

6.1.1.4 Human Intervention

This feature presents a very conflicting view in terms of ethical analysis in regard with GDPR. Article 22 contains the implications of a very important ethical attribute i.e. fairness. It states that every individual have a right to put a claim about not being judged by any kind of automated decision e.g. AI (Artificial Intelligence), machine learning algorithms etc. regarding data collection, processing or distribution and any other decisions made out of it. Moreover, subject can claim a human intervention regarding any such decision-making process which could affect the subject morally or legally [87].

Although Article 22 emphasizes on the fact that any such decision that could significantly affect the subject must be based on human intervention rather than having its completion solely by automated assistances, and that is how this article implies fairness. But one argument in favor of automation is that it removes human bias out of it consequently pushing the fairness towards more transparency. Similarly, a trained algorithm can eradicate the possibility of false negative or false positives to a significant extent consequently enhancing efficiency as well. In short, decision making through automated algorithms implies Deontological way of thinking for judging any individual morally or ethically because algorithms works on some hard-coded principles pre-fed to them which forms the basis of their decision making process irrespective of any consideration or regard to human nature, behavior, reputation, expectations and any other humane attribute. On the other hand, it could become difficult to expect from an algorithm to explain the logic or criteria of judgment involved behind executing any decision about any certain individual consequently making it almost impossible to challenge the decision made by an algorithm. Moreover, one inaccuracy could lead to destroy the results repeatedly towards every individual consequently disturbing the entire decision-making process [89].

6.1.1.5 Accountability

It's a very broad terminology that could cover a wide range of situations depending upon the way it is being handled because in GDPR, this term has been used only for once while "Responsibility" could be seen in quite a frequent use. Accountability could be seen only in Article 5 (2) where it compels the data controllers to comply with the law in terms of processing any kind of collected data of an individual, group or masses. GDPR encourages the data controllers towards compliance by inducing the terms of "Lawfully" and "Fairly" consequently covering both the legal as well as ethical part in terms of data processing by shifting the responsibility on the shoulders of the surveilling or data collection authority [87].

Hence, GDPR is also more tended towards legality than morality or ethics. Moreover, it does not even directly consider ethical aspects instead it provides us with mere ethical implications which are not enough to cater various activities happening across the cyberspace. Therefore, there is a dire need to induce more specificity in GDPR in terms of ethics pertaining to cyberspace.

6.2 Culture & Ethics

Culture plays the most important part in shaping the social fabric of any society not merely in formulating ethical or moral values instead it influences political, religious and technological infrastructure and norms as well consequently presenting a dominating role in painting the picture of any society. It is a variable term which is region oriented, but it also receives influence from racial hierarchies, religions, population, and technology as well and vice versa. Similarly, cultural norms also effect the surveillance tendencies in any region.

While analyzing culture in terms of information regime, there are two terminologies that are primarily important i.e. Privacy and Intellectual Property which are further influenced by conceptual, institutional, and behavioral tendencies set by cultural norms of any society. This could be simply explained by over viewing different regions across the globe in general. Asian cultures e.g. China and Japan doesn't contain any sophisticated and specific concept focusing on individual privacy instead they are more inclined towards collective interests and that's how and that's why surveillance mechanisms in these two regions are much more intense and deeply rooted in their societies consequently changing the entire concept of privacy [90]. The state surveillance apparatus deployed in China are expected to be as intrusive as we came to know about USA after Snowden's Revelations with one difference at hand is that China holds more tight control over citizens in terms of freedom of speech and privacy than US. Publicly presenting the so-called Great Firewall of China[27] appears to be a source of cracking down subversive content of citizens, confining freedom of speech and invading privacy rights consequently endorsing more tightly controlled surveillance culture within the region [91]. That Great Firewall of China is basically an initiative which is a combination of legislative and technological measures whose purpose is to monitor the regulation of internet within China and to block certain foreign websites. Moreover, it also aims to monitor and slow down the cross-border internet traffic

In 2016, a law was passed in China which imposed series of demands on internet companies to enhance the state control over data access. According to that law, internet companies are bound to increase surveillance through their networks, and they must provide information to the state investigators whenever they demand (Refers to section 3.4.2: Case of Downstream Surveillance). They were also instructed to reduce user anonymity by giving access only to those users who registers with their real identities (Refer to section 3.3). Similar situations were claimed to be experienced in Japan and Thailand as well [90]. Even in terms of their native vocabulary, there are implications that reflects the cultural mentality of these regions towards surveillance and privacy. E.g. in traditional Chinese, Japanese and Thai languages, there is no hardcoded explicit word for privacy. Modern Japanese adopts an equivalent translation of word Privacy from English vocabulary i.e. "Puraibashii" that comes under the list of words having foreign origins [92]. But yes, Japanese have one word for "Private" which is "Watakusi" whose literal meaning is "Partial, secret and selfish" [93]. And this is an antonym of the word "Ohyake" which means "Public". Moreover, things that implies Watakusi are less worthy than things that are Ohyake. Similarly, in China, the famous word that could possibly be closest to the English word privacy is "Yinsi" but its literal meaning is "shameful secret" and it is being used for negative and shameful behaviors and things [90]. But some claims were seen that somewhere in early 2000s, this word adopted some allied meanings as well e.g. something people doesn't want to share, secret (shameful or not) etc. and that also happened possibly under the western influence [90], [94]. Similar cultural influences as in China are claimed for Thailand as well [90]. One thing needs to be made clear that privacy is a basic human right as stated above many times throughout this document by giving various references, that's why it must be respected, protected and supported irrespective of race, color, region, religion, cultural and gender differences.

The above paragraph contains Asian cultural difference to point out its effects on privacy and surveillance tendencies, and yet we cannot tag the entire continent under the same cultural values because even in Asia, there are many countries having entirely different cultural norms. Therefore, it is even difficult to tag any single continent

[27] https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

completely under same cultural values ethically unless or until there exists a unified international framework agreed equally by every country within that continent.

Similarly, if we analyze the concept of privacy and surveillance tendencies in Pakistan and India from cultural point of view, then situation would be entirely different. Unlike China and Japan, the concept of privacy in these two countries is not even considered important not merely because of cultural values but because of their national, economical, and technologically unstable situations. Unlike first world countries of Europe or America, technology has not yet been deeply rooted in Pakistani infrastructure due to which manual operational activities are still experienced around the country. Automation industry in technology, especially in IT still lags even to Indian technological advancements although both are third world countries. In contemporary society, we cannot tag culture as an individual and independent entity that could influence or shape the ethical norms instead technological advancements, international stance, financial and economic situation of the country and religion are all inextricably linked with culture which consequently altogether plays an important role in shaping the ethical values of any region in terms of privacy and surveillance tendencies. That is why culture holds the responsibility to a significant extent but not the entire responsibility can be shifted to its shoulders. E.g. in Pakistan, religion focusses more on individual privacy while cultural and social norms do not, due to which being private more than to a certain extent is perceived to be as something negative and alarming. So, in short, an individual does not own a right to decide his/her extent of privacy, but mostly social and cultural norms decide that extent consequently declaring the morality of that privacy. And in Pakistan, surveillance tendencies are mainly fulfilled through social media by hiring social media specialists. In recent years, the concept of CCTVs has been started getting popular especially at the public places like auditoriums, airports, shopping malls etc. Surveillance through technology is less in practice than surveillance through man power e.g. almost at every single public entrance, individuals have to go through physical checking, similarly even travelling to any other city, there are check points for physical checking of vehicles and individuals while this things doesn’t happen in Europe and in many first world countries. In Europe, even while crossing the borders of some countries by road, sometimes, we do not get to see a check post even while in Pakistan, there are check posts even at the border of almost every major city. But such check posts cannot be blamed merely because of cultural concerns but because of security reasons which caused due to terrorism activities in last decade. Although terrorism has been taken down by security forces, yet we experience check posts for the purpose of sustaining security concerns.

Hence, culture can be considered as one of the many basic elements that could influence the privacy concerns and surveillance tendencies of any society, government and private organizations, yet we cannot solely blame this attribute for shaping the ethical norms of any society in terms of surveillance and privacy. Moreover, culture is a relative term which is subject to regional differences.

Conclusion

Although mass surveillance came under the limelight since the Snowden's revelations yet we haven't witnessed any kind of limitations that have been set in this regard nor we have experienced any accountability of any actor involved in it so far. Or even if there are any limitations been set, those are merely confined within documents which does not suffice the needs of user's privacy concerns.

Digital era Panopticism was contradicting Bentham's concept of Panopticon since before Snowden's revelations. It is because, current panopticons are trying to keep themselves being hidden and doesn't want the users to even know that whether they are under surveillance or not which distorts the whole concept of a Panopticon, but Snowden's revelations actually resolved this issue and now masses are conscious about being watched by an anonymous watchmen who isn't visible at all consequently satisfying the core concept of a Panopticon. Surveillance has become a flaming concern for every majority of the individuals who are connected to internet somehow. But an average internet user is still unable to figure out ways of maintaining his/her privacy while floating on the surface layer of the internet whereas few expert users sometimes manage to hibernate themselves under the deep web and dark web consequently making themselves not completely undetectable but to a significant extent, they manage to become untraceable. As explained above the necessity is the mother of invention and frequently experienced mass surveillance activities across the globe both by governments as well as by private organizations have compelled the individuals to find insidious ways for sustaining their privacy concerns. Therefore, contemporary society has left internet users with no choice but to adopt anonymity because concept of privacy is being tarnished somehow across every internet platform. In this thesis, after exploring all the possible actors involved in mass surveillance activities, it has been concluded that the actors involved in this activity could be i.e. Government Agencies (Or Intelligence Community), Private Organizations (Social media giants, data collectors, data aggregators, advertisers etc.), and certain individuals or groups. Government and Private organizations could be linked with each other depending upon the needs. But all the sub-actors as a part of private organizations are always linked because they are involved in capitalization of user data through a secure and insidious sale/purchase among themselves and their connections with each other is mandatory in order to keep running the economics of their business activities.

Considering only USA's case study in this thesis is because, majority of the internet companies having global access are Americans which ultimately makes America as a dominant country in terms of ownership of internet oriented companies and services consequently putting more responsibility on its shoulders as well as it gives USA more and more ways of sneaking into the internet without being identified.

An average internet user has to go through many hurdles in order to protect his/her privacy while surfing the internet and even after succeeding in securing his/her privacy against cookies, the option of device fingerprinting still remains at the hand of surveilling authorities. Hence, all these situations have enhanced the fragility of privacy due to which it can be ripped in many ways very easily by many actors sitting at the back of internet infrastructure. So, the word Panopticon does not merely imply the private and government companies instead it includes every single entity who is involved in any kind of surveillance activities while fulfilling the criteria of Bentham's conceptual Panopticon.

There are many laws available which considers privacy as a basic human right, yet we experience its violations in our routine life internet usage in the name of forced consents, permissions and so much more. And it implies that almost all such laws merely covers the generalized concerns about individual privacy, but over the time the surveillance techniques as well as internet usage and size have evolved to an enormous extent consequently changing the meaning of privacy concerns entirely. That's why there is a need to re-design all the previously available laws so that they could address every single issues concerning mass surveillance and privacy and at the same time could help in maintaining a balance as well between security and privacy. Majority of the laws available across the globe are more about legality and less about morality consequently not having any explicit framework of clauses based on ethics or morals except few legislations which implies ethics in few fragments while lacking any solid ethical considerations.

Many globally accepted frameworks declare privacy as a basic human right, yet it does not highlight the way it is getting breached consequently not highlighting the root cause of privacy violations specifically e.g. fingerprinting, cookie detection mechanisms etc. Moreover, current era's Panopticism and user privacy concerns does not just need any kind of documented ethical framework instead there is a need to deal this issue on technical scale as well. And this is the core reason due to which not a single such actor has been brought to justice and even if anyone came up to the court, they would slip away easily from every court prosecutions because there is no such legislations which could address every single privacy issue individually and specifically up to the core not just form legal view point but from ethical view point as well.

Utilitarian thinking proved to be quite a useful framework in analyzing mass surveillance from three perspectives, i.e. surveillant, surveilled and Edward Snowden. According to the findings of this thesis, it declares morality or ethicality of Mass Surveillance as a variable factor which depends upon various conditions if and only if those are fulfilled, Mass Surveillance is ethical otherwise not. The analysis raised some questions which must be answered before executing any surveillance activity. Those questions just represent an infant phase with an urge to fully develop any such framework by addressing more and more such questions so that the morality of any surveillance apparatus could be measured more precisely.

Mass surveillance as an activity cannot be directly tagged as unethical or illegal instead both the morality and legality of such activities predominantly depends upon the ways through which they are being carried out, that's why there is a dire need to focus on the ways which are in practice by various state and non-state actors.

Law and Culture, both are an equally important entities to shape and run any society in a systematic order being free from chaos. Morality of any society is predominantly influenced by its cultural norms which are always deeply rooted in any society irrespective of other allied factors. Culture and law are intertwined from ethical point of view and they invoke their dominance over one another under different circumstances in different times. But still, none of these two entities can be preferred over the other one because not every crime is Unethical and not every Ethical Act is Legal. The example of a hacker in a nuclear facility (Given in Section 5.2) ardently endorses this fact. That is why, in contemporary society, it has become practically impossible to divert the social setup completely towards one side while neglecting the other. Hence, instead of trying to segregate legality and morality, we need to give them their respective positions in society and instead of creating a comparison or competition between them, there is a need to make them supportive for each other so that every possible act followed by its consequences could be judged both on moral and legal basis.

References

[1] https://dictionary.cambridge.org/dictionary/english/ethic.

[2] Asma Jamal, Amber Ferdoos. Cyber-Ethics and the Perceptions of Internet Users: A Case Study of University Students of Islamabad.
Link:http://pu.edu.pk/images/journal/pjlis/pdf/2nd%20Paper%20-%20Vol%2016%20(2015)%20-%20Asma.pdf

[3] WESTMINSTER PAPERS in communication and culture VOLUME 9 / ISSUE 2 / APRIL 2013 The role of social media in the Arab uprisings – past and present.
Link:https://www.researchgate.net/publication/316087357_The_role_of_social_media_in_the_Arab_uprisings_-_past_and_present

[4] Ronald L. Jackson II, Darlene K. Drummond, & Sakile Camara. What Is Qualitative Research? Qualitative Research Reports in Communication Vol. 8, No. 1, 21 — 28. 2007.
Link: Link: http://dx.doi.org/10.1080/17459430701617879

[5] Sharlene Hesse-Biber. Qualitative Approaches to Mixed Methods Practice. DOI: 10.1177/1077800410364611
Link: https://journals.sagepub.com/doi/abs/10.1177/1077800410364611

[6] Paul Atkinson, Amanda Coffey, Sara Delamont. A debate about our canon, Qualitative Research by (2001). P:5-21

[7] David Collier. Understanding Process Tracing, University of California, Berkeley. doi:10.1017/S1049096511001429
Link:https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/understanding-process-tracing/183A057AD6A36783E678CB37440346D1

[8] Dr. Kenneth Harling, Wilfrid Laurier. An Overview of Case Study, University of Waterloo, Ontario, Canada.
Link:https://www.researchgate.net/publication/228472520_An_Overview_of_Case_Study

[9] https://www.helloitsliam.com/2018/08/31/surface-deep-and-dark-webs-whats-the-difference/.

[10] Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler. Below the Surface: Exploring the Deep Web by Forward-Looking Threat Research Team.
Link: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

[11] https://dictionary.cambridge.org/dictionary/english/panopticon

[12] https://plato.stanford.edu/entries/utilitarianism-history/ (Section 1-2)

[13] Julie Leth Jespersen, Anders Albrechtslund, Peter Øhrstrøm, Per Hasle and Jørgen Albretsen. Surveillance, Persuasion, and Panopticon, Aalborg University, Denmark.
Link:https://vbn.aau.dk/ws/portalfiles/portal/14102841/PerHasle_P07_article2.pdf
And www.researchgate.com

[14] Anne Brunon-Ernst. Beyond Foucault: New Perspectives on Bentham's Panopticon by Université Panthéon-Assas Paris 2.

Link:https://www.researchgate.net/publication/263007588_Beyond_Foucault_New_Perspectives_on_Bentham's_Panopticon

[15] Foucault, M.: Surveiller et punir: naissance de la prison, Paris, Gallimard (1975). P 200 - 220.

[16] Donna Susan Mathew. Surveillance Society: Panopticon in the Age of Digital Media.
Link:https://www.researchgate.net/publication/335208381_Surveillance_Society_Panopticon_in_the_Age_of_Digital_Media

[17] Christopher W. Hughes (1998) Japan's Aum Shinrikyo, the changing nature of terrorism, and the post-cold war security agenda , Global Change, Peace & Security, 10:1, 39-60.
Link:https://warwick.ac.uk/fac/soc/pais/people/hughes/researchandpublications/articles/japans_aum_shinrikyo_the_changing_nature_of_terrorism_and_the_post-cold_war_security_agenda.pdf

[18] https://www.9-11commission.gov/report/911Report.pdf

[19] Md. Rezaul Karim. Race to the Online Mass Surveillance: The End of Privacy and Open internet?
Link:https://www.researchgate.net/profile/Md_Karim73/publication/324659337_Race_to_the_Online_Mass_Surveillance_The_End_of_Privacy_and_Open_Internet/links/5b7a59e04585151fd1219bab/Race-to-the-Online-Mass-Surveillance-The-End-of-Privacy-and-Open-Internet.pdf

[20] https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[21] Jared Naude and Lynette Drevin. The adversarial threat posed by the NSA to the integrity of the internet, Computer Science & Information Systems North-West University Potchefstroom, South Africa.
Link:https://www.researchgate.net/publication/308733998_The_adversarial_threat_posed_by_the_NSA_to_the_integrity_of_the_internet

[22] David Lyon. The Snowden Stakes: Challenges for Understanding Surveillance Today, the Surveillance Studies Centre, Queen's University, Canada.
Link:https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_stakes/stakes

[23] David Lyon. Surveillance, Snowden, and Big Data: Capacities, consequences, critique.
Link: https://doi.org/10.1177/2053951714541861

[24] Sergei BOEKE. Reframing 'mass surveillance, Institute of Security and Global Affairs, Leiden University, the Netherlands.
Link:https://www.researchgate.net/publication/320740745_Reframing_'Mass_Surveillance'

[25] S.D. Warren and L. D. Brandeis, The Right to Privacy, *Harvard Law Review* 4, no. 5 (1890), 193–220, doi:10.2307/1321160.
Link:https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[26] European Court of human rights - Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home, and correspondence.

[27] THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND THE SEPARATION OF POWERS by Scott A. Boykin(Assistant Professor of Political Science, Georgia Gwinnett College, Lawrenceville, Georgia; Ph.D., Tulane University; J.D., University of Alabama School of Law; B.A., University of Alabama at Birmingham).
Link:https://www.researchgate.net/publication/302877717_The_Foreign_Intelligence_Surveillance_Act_and_the_Separation_of_Powers

[28] https://www.telegraph.co.uk/technology/2018/11/03/dozens-us-spies-killed-iran-china-uncovered-cia-messaging-service/

[29] https://www.businessinsider.com/how-china-found-cia-spies-leak-2018-8?r=US&IR=T

[30] M. Cayford, C. van Gulijk & P.H.A.J.M. van Gelder (*Delft University of Technology, Delft, The Netherlands).* All swept up: An initial classification of NSA surveillance technology.
Link:https://www.academia.edu/33095038/All_swept_up_An_initial_classification_of_NSA_surveillance_technology

[31] National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, 2015.
Link:https://www.nsa.gov/Portals/70/documents/about/civil-liberties/resources/BulkCollectionofSignalsIntelligenceTechOptions.pdf

[32] Jeramie D. Scott. Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space.
Link: https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/

[33] Helen Nissenbaum. Toward an Approach to Privacy in Public: Challenges of Information Technology University Center for Human Values Princeton University.
Link:https://nissenbaum.tech.cornell.edu/papers/toward_an_approach.pdf

[34] Introducing surveillance studies by David Lyon, Kevin D. Haggerty and Kirstie Ball, Routledge handbook of surveillance studies. Abingdon, UK: Routledge. By Marx G.T(2012). P (1-107). ISBN: 978-0-415-58883-6 (hbk). ISBN: 978-0-203-81494-9(ebk)
Link:https://www.academia.edu/6778392/Routledge_Handbook_of_Surveillance_Studies

[35] GLOBAL CHILLING: The Impact of Mass Surveillance on International Writers, Results from PEN's International Survey of Writers January 5, 2015.
Link:https://www.penmelbourne.org/wp-content/uploads/2019/08/GlobalChilling-PENInternational.pdf

[36] Elena Șușnea, Adrian Iftene.The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT) MFOI'2018, July 2-6, 2018, Chisinau, Republic of Moldova.
Link:https://ibn.idsi.md/sites/default/files/imag_file/230-240.pdf

[37] Robin Mansell (Editor-in-Chief), Peng Hwa Ang (Editor-in-Chief). The international encyclopedia of digital communication and society by. ISBN: 978-1-118-29074-3.

Link:https://books.google.fi/books?id=SVmsCQAAQBAJ&pg=PA1123&lpg=PA1123&dq=%E2%80%9CYour+papers+please%E2%80%9D:+Personal+and+professional+encounters+with+surveillance.+In+K.+Ball,K.+Haggerty,+%26+D.+Lyon+(Eds.),Routledge+handbookof+surveillance+studies(pp.+xx%E2%80%93xxx).+Abingdon,+UK:Routledge.+By+Marx+G.T(2012)&source=bl&ots=6qiO040z8c&sig=ACfU3U2mUSUXe5Pe4Bz0inJmSOchaU5F0g&hl=en&sa=X&ved=2ahUKEwirsYW-offpAhXRpIsKHTdwC6oQ6AEwAHoECAsQAQ#v=onepage&q&f=false

[38] Glenn Greenwald. No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State. Linkhttps://we.riseup.net/assets/201713/No+Place+to+Hide+Edward+Snowden%2C+the+NSA+and+the+Surveillance+State+Glenn+Greenwald.pdf

[39] David Greene, EFF Senior Staf Attorney Katitza Rodriguez, EFF International Rights Director. NSA Mass Surveillance Programs: Unnecessary and Disproportionate Link:https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf

[40] PRISM/US-984XN Overview OR The SIGAD Used Most in NSA Reporting. Overview PRISM Collection Manager, S35333 April 20L-3(Document leaked by Edward Snowden) Link:https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH9cc7.dir/doc.pdf

[41] https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[42] Izzat Alsmadi. The NICE Cybersecurity Framework: Cybersecurity Intelligence and Analysis. Springer; 1st ed. 2019 edition (January 24, 2019). P. 100-110.

[43] Michael Geist. Law, Surveillance and Privacy in Canada in Post Snowden Era. University of Ottawa Press (2015). ISBN 978-0-7766-2183-8 (pdf). Chapter 1. Link: https://library.oapen.org/bitstream/id/1b01cf32-192b-42a8-969c-381972eb8b4e/569531.pdf

[44] Andrew Clement (2014). NSA Surveillance: Exploring the Geographies of Internet Interception. In *iConference 2014 Proceedings* (p. 412–425). doi:10.9776/14119.

[45] Andrew Clement. IXmaps–Tracking your personal data through the NSA's warrantless wiretapping sites, Faculty of Information, University of TorontoToronto, Canadaandrew.clement@utoronto.ca.

[46] James Bamford. The Shadow Factory: The Ultra Secret NSA from 9/11 to the Eavesdropping on America. New York: Doubleday (2008), p. 289.

[47] (S//SI) FAIRVIEW AND STORMBREW: 'LIVE' - ON THE NET: LINK: https://www.aclu.org/node/59527 (document leaked by Snowden)

[48] NSA-project-X-intercept-16-1116.pdf :

link:https://cryptome.org/2016/11/nsa-project-x-intercept-16-1116.pdf (document leaked by Snowden)

[49] BLARNEY TEAM PROVIDES OUTSTANDING SUPPORT TO ENABLE UN SECURITY COUNCIL COLLECTION:
Link:https://www.aclu.org/foia-document/blarney-team-provides-outstanding-support-enable-un-security-council-collection (Document leaked by Snowden)

[50] BLARNEY EXPLOITS THE SOCIAL NETWORK VIA EXPANDED FACEBOOK COLLECTION.
Link:https://www.aclu.org/foia-document/blarney-exploits-social-network-expanded-facebook-collection - Document leaked by Snowden

[51] OAKSTAR: INTERNATIONAL COOPERATION.
LINK:https://www.aclu.org/foia-document/oakstar-international-cooperation (Document leaked by Snowden)

[52] https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

[53] The FISA Amendments Act: Q&A, The Intelligence Community's top legislative priority for 2017 is reauthorization of the FISA Amendments Act.
Link:https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf

[54] US PATRIOT ACT: SUNSETS REPORT.
LINK: https://www.justice.gov/archive/olp/pdf/sunsets_report_final.pdf

[55] F. Roesner, T. Kohno, and D. Wetherall, "Detecting and defending against third-party tracking on the web," in Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 155–168. [Online].
Link:https://www.usenix.org/system/files/tech-schedule/nsdi12_proceedings_full.pdf

[56] Web Application Security: A beginner's guide, Chapter 5: Browser Security principles: The same-origin policy.

[57] Panagiotis Papadopoulos Brave software panpap@brave.com, Nicolas Kourtellis Telefonica Research, Spain (nicolas.kourtellis@telefonica.com), Evangelos P. Markatos FORTH-ICS, Greece arkatos@ics.forth.gr. Cookie Synchronization: Everything You AlwaysWanted to Know but Were Afraid to Ask. Link: https://arxiv.org/pdf/1805.10505.pdf

[58] Dumas and Schwartz. Principles of Computer Networks and Communications. Upper Saddle River, NJ: Pearson Prentice Hall.

[59] Sylvia E Peacock. How web tracking changes user agency in the age of Big Data: The used user.
Link: https://journals.sagepub.com/doi/pdf/10.1177/2053951714564228

[60] Tomasz Bujlow, Member, IEEE, Valentín Carela-Español, Josep Solé-Pareta, and Pere Barlet-Ros. Web Tracking: Mechanisms, Implications, and Defenses
Link:https://www.researchgate.net/publication/280590332_Web_Tracking_Mechanisms_Implications_and_Defenses

[61] Nasir Muhammad M00421706 MSc. Tracking and Identifying Individual Users in a Web Surfing Session Computer and Network Security Middlesex University, London nm1066@live.mdx.ac.uk.
Link:https://www.academia.edu/4214725/Tracking_and_Identifying_Individual_Users_in_a_Web_Surfing_Session

[62] Browser Fingerprinting: A survey by PIERRE LAPERDRIX, CISPA Helmholtz Center for Information Security, Germany NATALIIA BIELOVA, Inria Sophia Antipolis, France BENOIT BAUDRY, KTH Royal Institute of Technology, Sweden GILDAS AVOINE, Univ Rennes, INSA Rennes, CNRS, IRISA, France.
Link:https://www.researchgate.net/publication/332873650_Browser_Fingerprinting_A_survey

[63] Fingerprinting Guidance.
Link: https://www.w3.org/TR/fingerprinting-guidance/#passive-0

[64] HTTP State Management Mechanism. ISSN: 2070-1721.
Link: https://tools.ietf.org/html/rfc6265

[65] B Eggleston. Utilitarianism, University of Kansas, Lawrence, KS, USA.
Link: http://www.benegg.net/publications/Eggleston_Utilitarianism.pdf

[66] https://dictionary.cambridge.org/dictionary/english/utilitarianism

[67] https://www.britannica.com/topic/utilitarianism-philosophy

[68] Larry Chonko, Ph.D. Ethical Theories. The University of Texas at Arlington.
Link: https://www.dsef.org/wp-content/uploads/2012/07/EthicalTheories.pdf

[69] Ethics of Security and Surveillance Technologies: OPINION NO. 28 OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES by European Group on Ethics in Science and New Technologies to the European Commission. ISSN 1830-3595.
Link:https://www.academia.edu/22963499/2014_Ethics_of_Security_and_Surveillance_Technologies_EGE_OPINION_NO._28

[70] (U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden.
Link: https://fas.org/irp/congress/2016_rpt/hpsci-snowden.pdf

[71] Jonathan Oram. Balancing Surveillance between needs of Privacy and Rights: CCTV in Japan & England: 6. No Paper Discussion CALE.
Link:http://cale.law.nagoya-u.ac.jp/_src/sc567/CALE20DP20No.206-2011.08.22.pdf.

[72] Gary T Marx. Surveillance Studies, Massachusetts Institute of Technology, Cambridge, MA, USA 2015 Elsevier Ltd.
Link: https://web.mit.edu/gtmarx/www/surv_studies.pdf
Or International Encyclopedia of the Social & Behavioral Sciences, Second Edition, Volume 23, 2015, 733–741.
Link: http://dx.doi.org/10.1016/B978-0-08-097086-8.64025-4

[73] The Global Surveillance Industry: A report by Privacy International July 2016.
Link:https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[74] https://www.boozallen.com/about.html

[75] Muel Kaptein en Johan Wempe. Three General Theories of Ethics and the Integrative Role of Integrity Theory. Link: www.Researchgate.com

[76] Neu, Michael; Dunford, Robin & Afxentiou, Afxentis (eds.) (2016). *Exploring Complicity: Concepts and Cases*. Rowman & Littlefield International, London, P. 20-30.
Link:https://books.google.fi/books?id=a-PaDwAAQBAJ&pg=PA26&lpg=PA26&dq=Either+you+were+complicit+with+the+project+or+you+were+the+enemy+of+the+project.+Exploring+complicity&source=bl&ots=TflQz5ShFj&sig=ACfU3U0R5nITPkk9ZhzSg5fmg5tRASqBSQ&hl=en&sa=X&ved=2ahUKEwjP1rmq7dbqAhVtsYsKHS5PADQQ6AEwAHoECAoQAQ#v=onepage&q=Either%20you%20were%20complicit%20with%20the%20project%20or%20you%20were%20the%20enemy%20of%20the%20project.%20Exploring%20complicity&f=false

[77] 'No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State', Independent Review, Volume 19, Number 4, pp. 605-609.
Reviewed by Michael C. Munger, Duke University. (Accessed Via jstor.org)

[78] Sean Michael Kerner. Snowden, NSA Disclosures Left a Changed World in Their Wake. June 06, 2014.
Link:https://www.eweek.com/security/snowden-nsa-disclosures-left-a-changed-world-in-their-wake

[79] Casey Hladik. Rusbridger's "The Snowden Leaks and the Public" and Mill's Utilitarianism: An Analysis of the Utilitarian Concern of "Going Dark".
Link:https://www.semanticscholar.org/paper/Rusbridger%E2%80%99s-%E2%80%9CThe-Snowden-Leaks-and-the-Public%E2%80%9D-and-Hladik/504d639194ccc6331dd43015ffa41a79e59bae8c

[80] https://plato.stanford.edu/entries/egoism/#EthiEgoi

[81] Martin Nwadiugwu. Consequentialist Theory. University of Nebraska at Omaha.
Link:https://www.researchgate.net/publication/283715974_Consequentialist_Theory

[82] Jonathan Riley. Mill's extraordinary utilitarian moral theory.
Link: https://doi.org/10.1177/1470594X09351952

[83] https://www.utilitarianism.com/mill2.htm , chapter 2.

[84] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT , Article 1.

[85] https://ethics.org.au/ethics-explainer-deontology/

[86] Antonio Pele, PUC-Rio University, Rio de Janeiro, Brazil. Roberto Andorno, University of Zurich, Switzerland. Human dignity DOI: 10.1007/978-3-319-05544-2_231-1. Link: www.researchgate.com

[87] https://gdpr-info.eu/

[88] http://web.mit.edu/gtmarx/www/ncolin5.html

[89] Tal Zarsky. The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. DOI: 10.1177/0162243915605575.

[90] Brey, P. (2007). ‘Is Information Ethics Culture-Relative?’ International Journal of Technology and Human Interaction. Special Issue Information Ethics: Global Issues, Local Perspectives. Guest ed. C. Ess. 3(3).

[91] The Road to Digital Unfreedom: President Xi's Surveillance State Xiao Qiang Journal of Democracy, Volume 30, Number 1, January 2019, pp. 53-67 (Article). DOI: https://doi.org/10.1353/jod.2019.0004

[92] Mizutani, M., Dorsey, J., and Moor, J. (2004). “The Internet and Japanese Conception of Privacy.” Ethics and Information Technology.
Link: scholar.google.com

[93] Nakada, M. and Tamura, T. (2005). Japanese Conceptions of Privacy: An Intercultural Perspective. Ethics and Information Technology.

[94] Lü, Yao-Huai (2005). Privacy and Data Privacy Issues in Contemporary China. Ethics and Information Technology.

[95] Joanna Lyn Grama (2014). Legal Issues in Information Security: Print Bundle (Jones & Bartlett Learning Information Systems Security & Assurance Series), 2nd edition. Chapter#2, p. 33-67

[96] https://plato.stanford.edu/entries/bentham/

[97] https://plato.stanford.edu/entries/mill-moral-political/#HapHigPle

Appendix – A

I have copy pasted Section 1.2 (Completely but with slight modifications), Section 2.1 and 2.2 from my own unpublished work (Research Article) so that's why these sections might increase my percentage of plagiarism because that unpublished work is also available on Moodle. My unpublished research article was a project of my Course named "Information Technology & Ethics 2019" which I submitted to Mr. Kai Kimppa (Turku School of Economics), hence he could be contacted as a reference person in case a confirmation of my unpublished work is required.

Appendix – B

The following article presents the objections posed on Mark Zuckerberg regarding privacy concerns on Facebook. The article presents thirty questions that are still unanswered by Mark Zuckerberg.

https://www.researchgate.net/publication/324819908_30_Questions_that_Facebook_has_yet_to_Answer_Gaps_in_the_testimony_of_Mark_Zuckerberg_at_a_US_Senate_hearing