Lund University
Department of Political Science

STVK02
Supervisor: Jonathan Polk

Digital Surveillance in the name of National Security

A Deontological, Consequentialist and Paternalistic interpretation of Edward Snowden's revelations in 2013

Bachelor's thesis (15 HP)

Jacob Kristiansson

January 5th, 2023

LUND UNIVERSITY

Abstract

Surveillance has throughout history been a widely discussed phenomenon and the debate over the delicate balancing of state power vis-à-vis privacy in the pursuit of national security equally so. In 2013, Edward Snowden revealed that the NSA had been conducting *digital* surveillance globally and it represents a tipping point in the history of surveillance. By applying the normative logics deontology and consequentialism, as well as the normative concept paternalism, an analysis has been made covering the reasonings and arguments behind both Snowden's and the National Intelligence Agencies' actions. This thesis has made visible how the logics and paternalism resonate both similarly and differently on the Snowden case. The research question was: *Can it be justified to allow national intelligence agencies to infringe upon their citizens' privacy through big data surveillance technologies in order to ensure national security?* Oversimplified, the conclusions are that the duty-ethical strand of deontology means that it cannot be justified, meanwhile for the rights-based strand of deontology, moderate deontologists and consequentialists, it is dependent on whether one values citizens' right to privacy or a state's end of ensuring national security higher. Paternalism, viewed through the utilitarian strand of consequentialism, means that it cannot be justified, as the NSA's paternalistic act cannot be deemed as exclusively rightful.

Key words: Normative Analysis, Deontology, Consequentialism, Paternalism, Edward Snowden, National Security Agency, Surveillance, Big Data, Intelligence, Disclosures.

Word count: 9996

Table of contents

1. Introduction

1.1. Background

Surveillance has become a widely discussed phenomenon in early modern history. In the 1850s, the glass architecture of the Crystal Palace in London and Les Halles in Paris became literary symbols of surveillance over citizens. Émile Zola criticised the political surveillance of the French Second Empire in *The Belly of Paris*[1], which itself was actuated by the construction of Les Halles. George Orwell wrote in his book *1984* (published 1949) that "(t)he Big Brother watches you", which portrayed the idea of a regime monitoring its citizens at all times. The debate over the delicate balancing of state power vis-à-vis privacy in the pursuit of national security has been historically recurrent.

That "the Big Brother is watching you" does not, however, seem to be merely present in classical literary works but in contemporary state practices. Hamid Ünver (2018, p.3) describes how China has implemented "police glasses that conduct real-time facial recognition analysis of citizens for law enforcement purposes" and how "Russia has SORM (System for Operative Investigative Activities) laws that allow full surveillance of analog and electronic communications without warrant." The recent advances in digital technologies have rendered it possible for *digital* state surveillance, rather than merely traditional physical espionage. Digital surveillance includes domains such as data security, geolocation, and biometrics (Ünver, 2018).

The United Nations Office of the High Commissioner for Human Rights (2013) wrote that the *UN resolution on the promotion and protection of human rights on the internet* in 2012 was "the first-ever UN resolution to affirm that human rights in the digital realm must be protected and promoted to the same extent and with the same commitment as human rights in the physical world." Since 2012, the discussion of human rights on the internet has intensified and evermore disclosures about state surveillance have been globally revealed. Edward Snowden revealed in 2013 that the United States conducted digital surveillance globally. The case occurred in a democratic state, without the citizens or the civil society being aware of the National Security Agency's (NSA) digital surveillance.

One could argue that there are numerous similar cases to that of Snowden's revelations, e.g., Chelsea Manning's leakages of classified military information in 2010 and Wikileaks' revelations in 2017 of the Central Intelligence Agency's (CIA) surveillance capabilities. The case of Edward Snowden's revelations is yet selected as the case represents a tipping point in the history of digital surveillance as it was the first disclosure of a widespread *digital* surveillance of citizens all over the globe. Edward Snowden (2020, p.3) tells the readers in his memoir *Permanent Record* that he possessed "unlimited access to the communications of nearly every man, woman, and child on earth who'd ever dialled a phone or touched a computer." Stefan Strauß (2018, p.59) writes that the software program *XKeyscore* allowed the NSA (where Snowden worked) to examine certain individuals' online communications. This

[1] Italics is used for titles of books or articles, to emphasise something for the reader (nota bene) or for concepts.

program is in turn an example of a *Big Data Surveillance Technology* (it is hereafter referred to as *BDST*).

Another example of a BDST is *PRISM*, which gave the NSA access to "tele- and Internet-traffic data from all the major service providers" (Gunhild Tøndel & Ann Rudinow Sætnan, 2018, p.204). The latter refers to major internet service providers, e.g., Facebook and Google. Moreover, Snowden helped the NSA to create a global backup (covert database) which would ensure that no data on global citizens' communication history was lost, hence the name *Permanent Record*.

The NSA took these precautionary measures following the 9/11 attacks. Snowden (2020) explains that the American Intelligence Community felt ashamed for failing to protect American soil and began therefore building a system which would secure that a similar attack would never occur again. However, the hunt for intelligence techniques would have privacy-mattered consequences.

1.2. Purpose and research question

The purpose of this thesis is to *understand* how the normative underlying logics *deontology* and *consequentialism* resonate differently on, as well as how the concept of *paternalism* can help us understand, the case-specific ethical dilemma of Snowden's revelations about the NSA's surveillance. The purpose is not to establish which logic provides the better answer.

The research question is the following:

- *Can it be justified to allow national intelligence agencies to infringe upon their citizens' privacy through big data surveillance technologies in order to ensure national security?*

The ethical dilemma ad hoc revolves around whether it is normatively justifiable or not, for National Intelligence Agencies (hereafter referred to as NIA) to infringe upon their citizens' privacy by using BDST in order to ensure national security. This thesis focuses on the case of Edward Snowden's revelations in 2013, to both limit the scope of this thesis and to better understand the implications of different normative arguments on this ethical dilemma. The research question puts an emphasis on a *state's* permitted or non-permitted technological means to reach the end national security, as the research question concerns the actions of NIA.

Nonetheless, that the emphasis is set towards a state's and NIA's actions is merely to broaden the scope of the question and thus increase the possibilities of generalising the findings of this thesis onto similar cases. *Both* the actions of NIA and the actions of Snowden will be the study objects. In order to understand this case, one needs to examine the perspectives of both actors, as they are interlinked. Detailed attention to merely one of these actors would not provide sufficient information, as one needs to gain a deeper insight of the reasonings behind the actions of both actors to see the whole picture.

The research question also directs its focus onto BDST, which is a subtype of surveillance, to further limit the scope. The usage of *surveillance technologies* was selected in order to make it possible for a wider generalisation of the study's results. Surveillance technologies refer to any digital technology that could have been or was able to serve the end of surveillance. Surveillance technologies could, however, be argued as too vague and thus, to clarify what is meant, big data can narrow it down.

According to Ann Rudinow Sætnan, Ingrid Schneider & Nicola Green (2018, p.2), big data serves as a "sociotechnical imaginary that serves as a meta-narrative to capture the present and future of digitisation, datafication, and globalised networks." Big data is furthermore widely used in academic works to gain intersubjectivity. It is utilised for both increasing the intersubjectivity and to serve as a meta-narrative to capture the general features of a globalised data network. From the collection and aggregation of big data through e.g., *XKeyscore* and *PRISM*, the NSA was able to extract privately held data for their end of ensuring national security. This makes BDST an integral aspect of the research question. A more precise definition on BDST is provided in the operationalisation section.

What sort of case can be deemed relevant for the times we live in? This is an example of a *so-what* question, which is necessary to answer for gaining external validity for normative analyses (Björn Badersten, 2006, p.192). A report about the issue of growing international threats to peoples' privacy was recently released by OHCHR (2022). The report mentions how the abuse of intrusive hacking tools by state authorities and the wide-spread monitoring of public spaces may increase the risk for violations of the human right to privacy in the near future (OHCHR, 2022). The case of Snowden's revelations in 2013 can be deemed relevant for the times we live in, as it represents a tipping point in the history of states' digital surveillance.

The Snowden case demonstrates the debate's relevance concerning the rightful balancing of state power vis-à-vis privacy in the pursuit of national security. Furthermore, it offers valuable insights on the general tensions (conflicts) between the theoretical normative logics of deontology and consequentialism. In brevis, deontology's primary focus lies on the rightfulness of an isolated act, rather than its consequences. In contrast, consequentialism targets an act's consequences as its primary point of departure. The concept paternalism can roughly be understood, according to Gerald Dworkin (1972, p.65), as "the interference with a person's liberty of action justified by reasons referring exclusively to the welfare, good, happiness, needs, interests or values of the person being coerced."

1.3. Literature review

All the articles and books mentioned below, constituting previous research on the topic, will be used in this thesis. One can better understand the discussion on the ethical dilemma by dissecting it into either evaluating the actions of Snowden (the leakages) or the actions of the state (e.g., by its data collection and surveillance) from a normative point of view. Moreover,

it could be analysed through either focusing on the actions themselves (deontology) or on the consequences of their actions (consequentialism).

Snowden (2020) explains that his memoir *Permanent Record* is about how his ethical principles led him to the decision of revealing the NSA's widespread surveillance. Moreover, he provides a discussion on the NSA's usage of BDST and how they functioned. In brevis, he asserted that a citizen's right to privacy should be valued higher than the NSA's end of ensuring national security. In a deontological manner, he argued that the end cannot justify the means. His arguments are necessary to analyse as they can make visible certain deontological reasonings, which is necessary to examine in order to fulfil the purpose of this thesis.

Marshall Erwin was an intelligence specialist at the Congressional Research Service where he played an essential role in shaping the congressional response to the NSA's surveillance leaks and is a non-residential fellow at the Center for Internet and Society at Stanford Law School (Just Security, n.d.). Erwin's (2014) research paper *Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection* analyses the consequences of the NSA's BDST. In particular, he examines the effectiveness of the bulk phone records collection, which was made possible through section 215 of the U.S. Patriot Act. To fulfil the purpose of this thesis, his analysis must be added as it will help to make visible consequentialist reasonings on this particular case.

Demelza Hays' (2015) article *The Ethics of Government Surveillance: Is Edward J. Snowden a Hero or a Villain?* provides a discussion on the morality of Snowden's actions. Hays (2015) analyses them through the normative logics (in similarity to this thesis) deontology and consequentialism. Despite the fact that she does not assess the NIA's actions, her discussion on the morality of Snowden's actions provides necessary insights for my thesis, as it revolves around whether to uphold privacy rights or ensure national security.

The Politics of Big Data: Big Data, Big Brother? was published by Routledge Research in Information Technology and Society in 2018 and offers academic viewpoints on the phenomenon of big data and its consequences on society in large. For instance, Stefan Strauß writes about *XKeyscore* and *TrapWire* (BDST) in the book, which will help evaluating the impacts of these technologies on citizens' privacy. Strauß is a Post-doctoral Researcher at the Vienna Institute of Technology Assessment (Austria). Ann Rudinow Sætnan explains the concept of big data and how *PRISM* (BDST) functions. She is Professor of sociology at the Norwegian University of Science and Technology in Trondheim (Norway).

2. Theoretical perspectives

This thesis will apply the normative logics of *deontology* and *consequentialism* to this case and include the normative concept *paternalism*. Trying not to entirely dichotomize the two normative logics is necessary for nuancing the debate. Hopefully, paternalism will be instrumental in this pursuit. A problematisation will be made in this section, as what is the most desirable outcome is heavily normatively debated.

Deontology and consequentialism were selected, as they constitute each other's antithesis and thus will provide contrasting angles on this ethical dilemma. Through opposing perspectives, it will be clearer for the reader how various normative logics provide different answers on this ethical dilemma and what the relationship between the logics' perspectives might be. Furthermore, it might display both differences and similarities between the two logics. The perspective of paternalism might deepen the discussion.

2.1. Deontology

Torbjörn Tännsjö (2000) writes that according to the ethics of deontology, certain acts are prescribed (good) or forbidden (evil), regardless of their consequences. Furthermore, human beings should not merely be used as means to an end but need to be treated as ends in themselves. Badersten (2006, p.110) explains that deontology's point of departure is the isolated act, which in turn is assessed on the basis of pre-established rules or duties. In addition, Badersten (2006) writes that the normative arguments of deontology are founded on pre-established values or principles which under any conditions should be regarded as inviolable and thus should be safeguarded at all times.

Nonetheless, the deontological logic itself never specifies the *exact* values, duties or rights that should be regarded as good or as inviolable. Deontology only provides an answer on *how* to resonate in normative questions, not on *what* should be justified. It mainly contends that the act itself should be the focal point in normative discussions. Thus, deontology lacks a value-substantial guidance and pre-established values are always dependent on what constitutes the moral subjects and/or the subject which establish the values (Badersten, 2006). There are two main-strands in deontology, and these contends differently about what acts should be regarded as good or evil. This thesis will include perspectives from *both* of these strands. They are not each other's adversaries, but rather complementary perspectives of deontology.

Tännsjö (2000) explains that the first strand is called *duty-ethics* and is based on Immanuel Kant's reasonings on the absolute duties of which one as a rule should not disobey. Amongst them is not to kill, lie or break vows. As they are non-good in themselves, they are forbidden. I.e., regardless of the acts' consequences. Additionally, according to Kant's Categorical Imperative, one should firstly "*only act accordingly to the maxim through which you can simultaneously seek that it become a universal law"* and secondly that one should "*always act*

so that you treat humanity, regardless of whether it appears in the form of yourself or in the form of another, as an end in itself, never exclusively as a means" (Tännsjö, 2000, p.61-63).

The other strand is the *rights-based ethics* and Badersten (2006) notes that certain acts are deemed forbidden as these would violate human rights if they were performed. For instance, The United Nations' (UN) declarations of human rights can provide answers on the question of what these rights may consist of. I.e., rights to freedom, state security and property. Meanwhile the duty-ethics maintain that the absolute duties and Kant's Categorical Imperative are sine qua non, the rights-based ethics cannot value e.g., a state's right to survival higher or lower than a citizen's right to privacy. This is due to the deontological logic *itself* not necessarily specifying the *exact* values, duties or rights which should be regarded as good or as inviolable.

The above leads us to the discussion of *value-conflicts* in the deontological ethics. As Badersten (2006, p.112) notes, if we both strive towards safe-guarding human rights (value) and strive towards safe-guarding the interests of a state (value), which sometimes could lead to violations of human rights, how should we then act? This is an example of a value-conflict in the deontological ethical-framework. The question is thus which particular duties or rights that should be regarded as more crucial than the other alternative. This is called value-hierarchy and the following question is an example of it: where do we draw the line for NIA's ambition to defend their state, concerning their justifications for infringement on privacy? It is a value-hierarchy as either the value security could be prioritised above privacy or vice versa.

The reasonings of deontology does not only involve individuals' rights or duties, where individuals are considered the moral subject, but groups as well (Badersten, 2006). Groups can consist of e.g., organisations such as the UN and states. Therefore, Badersten (2006, p.111) holds that for instance the principle of a state's right to survival and self-defence can be considered an appropriate moral subject for deontological discussions.

2.2. Consequentialism

Badersten (2006) writes that consequentialism assesses an act's moral substance after its' consequences. Consequentialism aim towards always creating as good consequences as possible for all people concerned (Tännsjö, 2000, p.32). In contrast to deontology, consequentialism means that acts are neither good nor evil in themselves. Rather the consequences of certain acts can be deemed as good or evil. The end can de facto justify the means, if the end is deemed to be of good character (Badersten, 2006).

However, in similarity with deontology, consequentialism lacks a value-substantial guidance. Consequentialism gives an answer on *how* to resonate in normative discussions, not on *what* should be justified (Badersten, 2006, p.117). However, meanwhile the deontological duty-ethics is founded upon pre-established values or principles which should be regarded as

inviolable, there are no such principles that consequentialism heavily strives towards. What should be regarded as good consequences and what values that should be aimed for when calculating what is the most desirable outcome of certain acts is subjective (Badersten, 2006). As Badersten (2006) explains, someone might value privacy as the worthiest factor to consider when dealing with a moral dilemma, meanwhile others might seek to defend the interests of a state.

Comparatively to deontology being tantamount to Kant's *duty-ethics*, *utilitarianism* is merely another expression of consequentialism. According to Tännsjö (2000, p.25), utilitarians resonate through a framework of what on the one side should be regarded as rightful and on the other as non-rightful. Tännsjö (2000) further explains that a rightful act merely should be perceived as *allowed* if the act is performed, not necessarily as an act which *should* be performed. In line with the *normative concepts-analysis*, the concept of *a rightful act* should only be regarded as rightful (and defined as such), *only* if there is no other available option that would provide better consequences. Moreover, we cannot *avoid* performing a rightful act, if it is perceived as an act that *should* be performed (Tännsjö, 2000, p.25-26).

2.3. Paternalism

Meanwhile paternalism is a normative concept and not a logic, it is necessary to include it as paternalism can offer valuable insights to that of the perspectives of deontology and consequentialism as well as increase this normative discussion's depth. One could view paternalism in two ways, as a subject either being *aware* or *unaware* of a paternalistic intervention.

As earlier established in section 1.2, paternalism can roughly be understood as "the interference with a person's liberty of action justified by reasons referring exclusively to the welfare, good, happiness, needs, interests or values of the person being coerced" (Dworkin, 1972, p.65). Nonetheless, paternalism does not only involve interference with the liberty of action, but also freedom of information.

Allen Buchanan (1978, p.372) noticed the connection between action and information and defined *paternalism* as "interference with a person's freedom of action or freedom of information, or the deliberate dissemination of misinformation, where the alleged justification of interfering or misinforming is that it is for the good of the person who is interfered with or misinformed." This entails that a person can be deliberately misinformed by the entity that this person is subjected to, with the justification that it is for the person's own good. Dworkin (1988), however, meant that this definition of paternalism was too limiting, as paternalism may include non-coercive means to achieve an end. Dworkin was inspired by Bernard Gert and Charles Culver.

Gert and Culver (1976, p.48), wrote that "an essential feature of paternalistic behaviour toward a person is the violation of moral rules (or doing that which will require such violations), for example, the moral rules prohibiting deception, deprivation of freedom or opportunity, or disabling." Paternalism involves according to Gert and Culver (1976) a violation of a moral rule for achieving good outcomes for the person who is interfered with, regardless of the person's *consent*. Moral rules are interpreted ad hoc by the author as pre-established rules that a moral subject is supposed to respect and follow.

Both cited definitions, by Gert & Culver (1976) and by Buchanan (1978) will be used in this thesis. This is due to the former one explicitly mentioning the important relationship between action and information, and the latter one mentioning the crucial factor of violations of moral rules. These definitions are selected in order to limit the theoretical scope of the paternalistic concept.

Having the above reasonings in mind, an interference with a subject's freedom of action or freedom of information entails not only an obstruction of a subject's freedom of action, but also a procedure which obstructs a subject to even become *aware* of his or her available options of actions. This could be illustrated through for instance a state not informing its' citizens about their deprivation of rights, referring to their wellbeing.

It appears the paternalistic reasonings of intentions about good *outcomes* is compatible with the consequentialist way of reasonings, as consequentialists argues that an act is only wrong if the *consequences* of an act are evil. This reasonings would imply that a state de facto can, according to a consequentialist interpretation of the concept paternalism, take actions without the citizen being aware of it. Given that it would be a rightful act and that the consequences of the act are deemed good.

According to Tännsjö (2000, p.86), the deontological strand which is rights-based refutes the arguments of paternalism, as citizens have an absolute right to autonomy and non-interference in decision-making. However, Jason Hanna (2018, p.118) writes that "according to moderate deontologists such as Judith Jarvis Thomson, moral rights have thresholds beyond which they can be permissibly infringed." Hanna (2018) suggests that a right can be infringed if it would benefit the individual and that, in such case, a paternalistic intervention could be applicable. This makes the case that deontology also is compatible with paternalism.

2.4. Alternative theories

Other normative logics that could have been selected instead of deontology and consequentialism for this normative analysis are e.g., *contractualism* and *appropriateness* (or *circumstance*) *ethics.* Regarding *contractualism,* one would need to consider the socially constructed agreements or contracts between a state and its citizens (Björn Badersten, 2006). One could have proceeded with the Snowden case by for instance contemplating on to what

extent the American citizens are willing to trade their own decision-making in exchange for the U.S. intelligence agencies' protection of their lives and property. I.e., what the contract between the citizens and the U.S. state de facto would entail in terms of the limitations on privacy vis-à-vis state-provided security. Badersten (2006) explains that *appropriateness ethics* would instead consider the circumstances in a certain ethical dilemma. As for the Snowden case, a suitable question to ask could be what the circumstances were that led the NSA to conduct widespread digital surveillance, and how the NSA justified their violations of American citizens' privacy.

3. Method and material

3.1. Normative Method

The research question for this thesis is the following:

- *Can it be justified to allow national intelligence agencies to infringe upon their citizens' privacy through big data surveillance technologies in order to ensure national security?*

The ad hoc ethical dilemma is whether it is normatively justifiable for NIAs to infringe upon their citizens' privacy by using BDST to ensure national security or not. To answer this question and to limit the scope of this thesis, I have decided to apply the theoretical normative logics deontology and consequentialism, as well as the normative concept paternalism, to this case. The analysis will display certain conflicts between the different normative logics and the concept of paternalism will help provide further valuable insights on the case.

This thesis will answer the research question by primarily conducting a *given-that* form of normative analysis on the case of Edward Snowden's revelations in 2013 about the existence of mass intelligence gathering surveillance programs run by the U.S. National Security Agency (NSA). This method will provide vital theoretical tools for unveiling the conflicts between the selected normative logics and between the logics and the concept of paternalism. Nonetheless, even though I will mainly use the *given-that* – form of normative method, I will also make use of the *normative concepts-analysis* as a supplemental normative method, as it will make possible for a wider discussion on the theoretical definitions and altering meanings of the normative logics and concepts (Badersten, 2006, p.43). This will in turn help provide more depth to the overall normative discussion. More information about the different forms of normative methods will be provided later in this section.

There are several different methods that one could utilise in approaching this ethical dilemma, not merely the normative method. For instance, one could use the method of *the substance analysis of ideologies and political ideas*. Ludvig Beckman (2005, p.12) writes that a substance analysis of ideologies and political ideas views political messages as a collection of arguments which critically analyses the durability and validity of arguments. The intention of such an

analysis is to *test* and *criticise* the validity and durability of these arguments. (Beckman, 2006). An analysis like this may therefore, for instance, analyse the validity of the argument that allowing NIA to infringe upon their citizens' privacy is justified for ensuring national security. One could argue that what is then principally interesting is the *argument itself* and the durability of it, rather than understanding a statement's underlying logics or values.

Ludvig Beckman (2006) explains that the aim of the method of analysis called the *critique of ideas* (or *the critical analysis of ideologies and political ideas*) is to point out obscurities, inaccuracies and contradictions with various political arguments. Beckman (2006) further elucidates how the *critique of ideas* neither merely examines political parties' arguments nor classical political texts, but also examines the reasonings of state powers. Thus, perhaps the method of analysis *critique of ideas* would provide solutions to this thesis's ethical dilemma, as we then might be able to demonstrate the *durability* and *validity* of the various arguments. However, Ludvig Beckman (2006, p.331) contends that the aim of a normative analysis "is mainly to illuminate the implications and consequences of certain values and ideals - not to prove them." Therefore, one can conclude that the critique of ideas and normative analyses directs their attention to different ends. The former seeks to *prove* the validity of certain arguments and the latter not to prove, but to *understand* how different normative logics provide various arguments on a certain ethical dilemma. The latter will be the main aim of this thesis. For such a pursuit, the normative method is the most suitable one. There are three forms of analyses to choose from when using the normative method: the *given that*, the *normative concepts-analysis*, and the *normative analysis in the strict sense of the word.*

Badersten (2006) writes that a *given that* form of normative analysis conducts a comparison between and problematisation of different normative logics. It provides a methodological framework for comparing different views on values and makes visible how different normative views lead to various conclusions (Badersten, 2006, p.50). I will largely be using the given that – form of normative method, as I then will be able to ask the question: *given that* our point of departure is either the normative logic *deontology* or *consequentialism* or the concept *paternalism*, can the American NIA's actions be justified in this particular case?

It is the most suitable form of normative analysis for this thesis's aim and will therefore be the main theoretical approach in this thesis. Nonetheless, as previously established, this thesis will furthermore gain more depth by applying the *normative concepts-analysis*, as a supplemental normative approach. This is meant by the author to make it possible for a wider discussion on the theoretical definitions and altering meanings of the normative logics and concepts utilised in this thesis.

Another form of normative analysis is the *normative concepts-analysis*, which seeks to clarify the meaning of and the relationship between different values, normative logics, and normative concepts (Badersten, 2006, p.50). It also seeks to make visible possible *value-hierarchies* and to expose potential *value-conflicts* (Badersten, 2006, p.188). A value presents itself in the form of something which is deemed good or evil, desirable or non-desirable, as well as better or worse than something else. In the context of NIA and the justifications or protests against the

usage of BDST, e.g., the inviolable rights of humans, the right to privacy, and the interests of the nation are distinguished values in this normative debate.

In the context of NIA and BDST, discussions on e.g., the meaning of the concept privacy and how we should or could define it, would therefore be suitable for a *normative concepts-analysis*. It would be particularly interesting to examine where there might be a clash of interests between achieving both national security and privacy, by conceptualising both values. Furthermore, it would increase this thesis's intersubjectivity. Defining the value privacy will help answering the question: where do we draw the line for NIA's ambition to defend their state, concerning their justifications for infringement upon privacy? This is an example of a value-hierarchy, where the value security is prioritised above privacy or vice versa. Such an examination will be fruitful for this thesis's inquiries into the ethical dilemma between privacy vis-à-vis national security concerns.

The third form of normative analysis is the *normative analysis in the strict sense of the word.* The intention ad hoc is to justify a certain normative stance with a point of departure from a specified basis of value. I.e., to justify certain convictions on what is deemed desirable and in a rational manner argue for selected normative stances (Badersten, 2006, p.188). In the context of NIA and BDST, this could for instance entail justifying the actions that NIA took regarding BDST. Such an examination could too be fruitful for further research regarding this particular ethical dilemma as we then may understand the normative underlying logics or values behind such a justification.

However, I have decided not to use this form of normative method as it opposes the aim of this thesis. I will neither take a certain normative stance nor seek to justify particular normative convictions. I merely seek to *understand* how different normative logics provide various arguments on a certain ethical dilemma. It is possible for me to conduct a neutral analysis, as I will not seek to take a stance myself. Instead, I will explain how the different theoretical logics can view this ethical dilemma differently, from a value-free standpoint.

3.2. Operationalisation

In order to be able to answer the research question, one must disassembly it into key concepts and then operationalise and define these:

Being justified: in line with the normative method, by a justification is meant a normative logic's or concept's theoretical justification of a certain normative statement.

National Intelligence Agencies (NIA): government agencies that deals with national security issues, by collecting and analysing intelligence.

Infringe upon: "if something infringes on/upon someone's rights or freedom, it takes away some of their rights or limits their freedom" (Cambridge Dictionary, n.d.).

Privacy: "the quality or state of being apart from company or observation" and "freedom from unauthorized intrusion" (Merriam Webster Dictionary, n.d.).

- Therefore, the author means that infringement upon privacy is seen in this thesis as both (1) taking away some of someone's rights, e.g., the right to being apart from company or observation, and (2) to limit someone's freedom from unauthorized intrusion.

Big Data Surveillance Technologies (BDST): The definition of *big data* is according to Ann Sætnan, Ingrid Schneider & Nicola Green (2018, p.6): "the collection and aggregation of large masses of (publicly, commercially, proprietarily, and/or illicitly) available data and its analysis, largely in the form of correlation, pattern-recognition, and predictive analysis." As earlier mentioned, through e.g., *XKeyscore* and *PRISM*, the NSA was able to extract privately held data (by collecting large masses of data) for their end of ensuring national security. Surveillance technologies in turn refers to any digital technology that could have been or was able to serve the end of digital surveillance.

National Security: "the ability of a state to cater for the protection and defence of its citizenry." (Segun Osisanya, n.d.).

3.3. Material

The material that I will use for this thesis will both consist of primary and secondary sources. It is beyond the time limit of my thesis for conducting interviews and transcribing them, which could constitute additional primary sources. The material of this thesis will primarily consist of secondary sources and their normative discussions about the Edward Snowden case. These secondary sources will consist of academic articles and books, which will be targeted towards including both Snowden's normative arguments as for why he revealed the existence of the NSA's mass intelligence-gathering surveillance programs and the normative reasonings of the NSA for conducting such surveillance. The material will not be limited to merely examining the official arguments of the NSA and Snowden. I argue that it is possible for me to also include other sources that bring up the normative discussions about the Snowden case as what is principally interesting is *how* different normative logics can view this case in various ways. It is therefore not *necessarily* vital to distinguish *who* exactly argues what. Nonetheless, I will for instance use Snowden's autobiography Permanent Record from 2020, constituting a primary source for this thesis. In addition, I will e.g., utilise press releases through the official website of the NSA, in order to analyse the NSA's own official stances and arguments concerning Snowden's revelations.

4. Analysis

- Can it be justified to allow national intelligence agencies to infringe upon their citizens' privacy through big data surveillance technologies in order to ensure national security?

4.1. The normative logic of Deontology – The actions

Snowden (2020) argues both in line with 1) the *rights-based ethics* and 2) the *duty-ethics* strand of deontology in his memoir *Permanent Record*. For instance, Snowden (2020, p.6) argues that in defence of the U.S. constitution, for the end of benefitting the public, he had sworn an oath of service. He asserts that the constitution, which was supposed to guarantee civil liberties, had been "flagrantly violated" by the NSA's mass-surveillance (Snowden, 2020, p.6). Furthermore, he asserts that a state's limitations on violating citizens' privacy clearly demonstrates where and when "a government may not infringe into that domain of personal or individual freedoms that…. is called "privacy"" (Snowden, 2020, p.6-7).

4.1.1. Rights-based ethics

The rights-based ethical arguments of Snowden are continuously found through the pre-established values or principles, of which he deems should be perceived as inviolable. The pre-established principles which he chiefly stands for, are formulated through his defence of the U.S constitution.

Snowden (2020) explains that the constitution itself was constructed to guarantee civil liberties for the U.S. citizens and that the 4th Amendment in particular protects people and their property from government surveillance. Especially as it holds that "(t)he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue…." (Snowden, 2020, p.229). He asserts that, accordingly to his interpretation of the 4th Amendment, that without a specific warrant for the government to interfere with an individual's private matters or to intrude in a specific area of an individual's freedom, the government violates the citizen's privacy. According to Snowden (2020, p.207), "we have a single concept that encompasses all this negative or potential space that's off-limits to the government. That concept is "privacy"." What is essentially being asserted here by Snowden, is that neither privacy can be violated nor searches and seizures of personal property can be used as a means for a government's end, if there is no specific warrant for performing such an act. Regarding citizens' own data, Snowden (2020) holds that it should be deemed as legally protected personal property for the citizens in accordance with the 4th Amendment.

On a similar note, the philosopher Onn Yael (2005, p.12) writes that one should define the right to privacy as giving us "the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose". He holds that the right to privacy is meant to protect the autonomy of citizens from government interference, which includes the citizens' own control over the access of personal property.

The NSA's surveillance technologies and internal policies, however, disregarded the 4th Amendment, as the agency neither regarded data as personal property, nor deemed data collection as "searches and seizures" (Snowden, 2020, p.229-230). The NSA could have resonated in line with the normative standpoint that a state's right to self-defence should be considered the primary moral subject in this normative discussion. This would in turn entail that a state's right to self-defence against terrorism would be valued higher than a citizen's right to privacy. In this manner, the government could infringe upon their citizens' privacy as it would ensure the asserted more crucial value national security, despite the fact that citizens' privacy would serve as a means to the end of deterring terrorism.

Snowden, however, holds that civil liberties (especially the right to privacy), which ad hoc would represent the means, should be valued higher than the NSA's stated end of deterring terrorism. This is what both constitutes Snowden's asserted value-hierarchy and pre-established principles of which one should not violate. According to Snowden (2020), the government cannot infringe upon their citizens privacy, even if it would serve as a means to the end of deterring terrorism, and thus ensuring national security.

4.1.2. Duty Ethics

Snowden's (2020) duty-ethical arguments are seen through his acknowledgement that meanwhile terrorism was the stated cause of why the NSA created surveillance programs, serving as their main objective, the U.S. had instead during the decade starting from 9/11 in 2001 and ending in 2011 made the mass surveillance programs a larger threat to civilians' liberties rather than terror itself. Snowden resonate in a duty-ethical manner, as according to Kant's categorical imperative, one always need to act so that you treat humanity (i.e., citizens) as an end in itself and never exclusively as a means. This means that the citizens should not be exclusively treated as a means, through NSA's BDST technologies, to fulfil the end of national security.

Another aspect to the duty-ethical arguments, is that there are absolute duties of which one cannot, in any circumstance, disobey. One of the absolute duties concern not lying, and Snowden (2020, p.231) notes that former Director of National Intelligence (DNI) James Clapper in 2013 lied to the U.S. Senate Committee on Intelligence meanwhile he was testifying under oath. Clapper told the committee that the NSA did not collect data via American citizens' communications, at least not deliberately. Snowden (2020) argues, in line with the absolute

duties arguments by the duty-ethical strand, that Clapper should not have lied to the U.S. Senate about the NSA not collecting American citizens' data.

4.2. The normative logic of Consequentialism – The consequences

Consequentialism could argue that allowing NIA to use BDST technologies can be justified if it would entail ensuring national security, *even if* it would violate citizens' privacy. This is due to the consequentialist assertion that the end justifies the means. However, this standpoint assumes that ensuring national security is regarded as the most desirable end. The unclearness ad hoc is that it is not necessarily national security which would be on the top of the value-hierarchy. It could all the same be ensuring the citizens' privacy or autonomy.

What should be regarded as the most desirable consequences in the case of Snowden's revelations is dependent on a value-hierarchy, as either national security could be prioritised above citizens' privacy, or vice versa. In contrast to duty-ethics, there are no pre-established values or principles that consequentialism heavily strives towards. Hence, what values that should be aimed for when calculating what is the most desirable consequences of certain acts is subjective. Another challenge is that it is difficult to calculate and get an objective result concerning the effectiveness of the NSA's BDST technologies for preventing further terrorist attacks.

As the purpose of this thesis is to understand how the normative logics resonate in this case, one can still find relevance in examining how the different actors in this case contend differently. Actors such as the NSA or Snowden can either maintain that what is essential to emphasise are 1) the consequences of surveillance for national security, 2) the consequences of Snowden's leakages for national security or 3) the consequences of surveillance on privacy.

The NSA (n.d.) write on their official website that the Foreign Intelligence Surveillance Act (FISA) was created in 1978 to regulate what sorts of foreign intelligence collection that the NSA is legally permitted to gather. This intelligence collection includes surveillance techniques which the NSA get assisted with via U.S. telecommunications service providers. The NSA relies heavily on receiving warrants from the FISA court, for employing the necessary techniques for acquiring foreign intelligence information. The court was established in 1979 to ensure that the intelligence collection is done accordingly with the U.S. Constitution, including that of the 4th Amendment. FISA is "designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans" (NSA, n.d.).

Section 702 of the FISA was created in 2008 and it authorized the NSA to target non-American citizens via communication who are believed to be located outside the U.S. (NSA, n.d.). The intelligence collection involved, however, the communications of U.S. citizens, as they are according to the NSA (n.d.) "sometimes incidentally acquired in targeting the foreign entities."

For instance, this might entail an American citizen who is in contact with a terrorist suspect. In such cases, the NSA must receive a warrant given by the court, via consultations with the Attorney General and DNI, as a tool to protect the privacy of the American citizen. This is called a minimisation procedure, as it shall minimise the infringement upon privacy of American citizens (NSA, n.d.).

4.2.1. Consequences of surveillance for national security

As earlier mentioned, through the collection and aggregation of large masses of available data through PRISM, NSA got access to Internet-traffic data from all the major communication-service providers. According to the NSA (n.d.), section 702 has been of major importance for the "detection, identification, and disruption of terrorist threats to the U.S. and around the world." The NSA (n.d.) argue that the arrest of the terrorist Najibullah Zazi and his co-conspirators was made possible through the mass-collection of data, which in turn was thanks to section 702. In September 2009, the NSA found out that Zazi (at the time located in the U.S.) was in contact with Al Qaeda in Pakistan. The NSA (n.d.) writes that, once they realised that Zazi was planning to bomb the subway system in New York City, by tracking his communications, they arrested him. Later on, Zazi pled guilty to this scheme (NSA, n.d.).

On a similar note, about the importance of the FISA section 702, Marshall Erwin (2014) holds that the section has been effective in defending national security. The usage of PRISM was made possible through section 702 and Erwin (2014) holds that section 702 (representing the means) helped NSA to intercept emails from Zazi, which in turn was instrumental in identifying him (the end).

Erwin (2014) explains that Section 215 of the U.S. Patriot Act aided the NSA to centralise phone records of millions of U.S. citizens into one large data set. Erwin (2014) writes that the intelligence community held that if the NSA had section 215 at their disposal, then the 9/11 hijacker Khalid al-Mihdhar could have been apprehended and that the section was crucial in apprehending Zazi. However, Erwin (2014) argues that phone records collection through section 215 neither would have helped to hinder the 9/11 plot nor was essential in apprehending Zazi. He explains that section 702 (for intercepting emails) was sufficient for capturing Zazi. Regarding the 9/11 plot, Erwin (2014, p.7) writes that the "post-9/11 investigations show that the intelligence community had sufficient information about al-Mihdhar to disrupt the attack but not sufficient initiative, largely as a result of cultural barriers and other institutional impediments within different intelligence agencies". He maintains that the phone records collection was of marginal value in both cases (Erwin, 2014). The collection itself constitutes a BDST technology. Erwin (2014) means i.e., that section 215 has not served as a successful means to achieve the end national security, meanwhile section 702 has.

4.2.2. Consequences of Snowden's leakages for national security

The consequences of Snowden's leakages have been severe for the U.S.'s national security, according to former DNI Clapper and former Deputy Director of the NSA Richard Ledgett. Clapper claimed in January 2014 (Mark Mazzetti & David Sanger, 2014) that "Snowden's disclosures had done grave damage to the country's security and had led terrorist groups to change their behavior to elude American surveillance". The NSA (2014) published a press release about an interview with Ledgett at a TED conference, in which Ledgett stated that "(t)he actions that he took were inappropriate because of the fact that he put peoples' lives at risk, basically, in the long run" (NSA, 2014).

Regarding how exactly Snowden had put national security and people at risk, Ledgett mentions that the disclosures meant a decreased ability to have insight into the actions of terrorists. Moreover, Ledgett held that American diplomats, soldiers, military personnel and allies who find themselves in dangerous situations now are at greater risk, as the NSA are not able to see the potential threats that might appear (NSA, 2014). I.e., if the NSA does not have big data surveillance technologies to their disposal.

4.2.3. Consequences of surveillance on citizens' privacy

Through BDST, NIA can both work in a preventative and a directly deterring manner. Stefan Strauß (2018) writes that the BDST technology *TrapWire* was aiming at predicting terrorist attacks through large networks of surveillance cameras, that were linked to several databases which were being used by intelligence agencies in the U.S. (Strauß, 2018). Technologies such as TrapWire, infringe upon citizens' privacy. As infringement upon privacy is seen in this thesis as the right to being apart from observation, TrapWire infringes upon citizens' privacy as it is monitoring citizens' movements through surveillance cameras.

Furthermore, Strauß (2018) explains how XKeyscore represents another example of infringement on privacy as the NSA was able to examine individuals' online communications and their social media activities. He points out that privacy was regularly seen by intelligence agencies as "a burden to security" (Strauß, 2018, p.61). I.e., that privacy was dichotomous to security. Snowden (2019, p.195) holds that surveilling citizens on their property (he regards data as personal property) without a warrant are one of the most important prohibitions against law enforcement. That the NSA was surveilling citizens on their property without a warrant could be viewed as an unauthorized intrusion, which itself also constitutes an example of infringement upon privacy (see section 3.2).

4.3. The normative concept of Paternalism – The decision-making

As earlier established, paternalism can roughly be understood as "the interference with a person's liberty of action justified by reasons referring exclusively to the welfare, good, happiness, needs, interests or values of the person being coerced" (Dworkin, 1972, p.65). Furthermore, it entails an interference with a person's freedom of action or information, where a person's actions or *awareness* of his or her available options of actions are obstructed, for the sake of the person's welfare.

The *unawareness* of a subject's infringed privacy is particularly interesting in the case of Snowden's revelations, as the NSA took action on behalf of the American citizens, which would infringe upon their privacy without their knowledge. As Ross Bellaby (2018, p.197) explains, "Edward Snowden's revelations highlight a real lack of knowledge as to the abilities, willingness and drive had by the intelligence community to collect data *en masse*." Data "en masse" means ad hoc all data being collected by the intelligence community as a whole. As Snowden (2020) describes it, he could make decisions, without any supervision because of his computer knowledge and skills, on behalf of his fellow American citizens. He states that the NSA perceived their and Snowden's solutions, i.e., the BDST technologies, as naturally apolitical as they were based on data. Instead of the solutions being based on the limited knowledges of the common citizen, he means that the American intelligence community perceived itself as possessing solutions for everything and everyone, which in turn made them believe that they could act on behalf of the American citizens (Snowden, 2020, p.122). What was being asserted by Snowden (2020), is that neither privacy can be violated nor searches and seizures of personal property can be used as a means for a government's end if there is no specific warrant for performing such an act.

One can understand this phenomenon as a paternalistic act, made by the NSA, to ensure that their stated end of deterring terrorism was being pursued in order to secure the U.S.'s national security. The NSA acted on behalf of the American population, referring to their citizen's welfare, without the citizens being aware that their privacy was being infringed upon (as they had no knowledge about the NSA's actions) and without the NSA possessing a warrant for this action.

If a government would take measures that would infringe upon their citizens' privacy, taking this decision on behalf of its citizens, in order to secure their citizens' privacy, how would the field of discussion look like? Demelza Hays (2015) write that "(p)olicies that violate private property in order to protect private property, which is an example of a performative contradiction, are the result of an amalgamation of these ethical approaches." What she refers to when writing "amalgamation of these ethical approaches" is the combination of deontology and consequentialism. She means that this combination often constitutes modern ethics. Hays (2015) concretises this by writing that on the one hand "the government uses consequentialism to argue that the benefits of surveillance outweigh the costs of terrorism" and on the other that "the government uses deontology to claim that good actions are those that protect the property of Americans."

However, one could argue that it is not merely the combination of deontology and consequentialism that the American intelligence agencies were using to justify their actions, but their actions were also justified by paternalistic motives. Referring to the arguments unfolded in sections 4.2.1 and 4.2.3, it was held by Erwin (2014) that FISA section 702 has been effective in defending national security. Furthermore, the American intelligence agencies argued that if the NSA had section 215 to their disposal, then 9/11 might have been stopped and that *TrapWire* could predict terrorist attacks by gathering data from surveillance cameras. The American intelligence agencies have thus, one could argue, taken actions with the help of various BDST technologies, which would serve as means to the end of ensuring national security. These actions were done without specific warrants or by the consent of the American citizens, with the claim that it is for the sake of the citizens welfare.

5. Discussion

Neither the logic of deontology nor consequentialism specifies the exact values, duties or rights that should be regarded as good or as inviolable (value-substantially neutral). Deontology merely examines the isolated act itself and consequentialism the consequences of a certain act. Nonetheless, one can at least maintain that the deontological strand duty-ethics regards humanity as an end in itself and can never be used exclusively as a means. This entails that citizens and their privacy cannot be *exclusively* treated as a means, through BDST technologies, to fulfil a state's end of national security. This is what Snowden asserted.

Concerning the rights-based ethical strand of deontology, it is worth considering the value-hierarchy and the moral subject. If the latter concerns the individual citizen and the right to privacy is valued higher than a state's right to self-defence, then the rights-based ethics would reasonably maintain that it cannot be justified to allow NIA to infringe upon their citizens' privacy through BDST technologies in order to ensure national security. This is in line with the arguments of Snowden shown in section 4.1.1. If, however, the moral subject is the state's right to self-defence and if the value of a state's right to security is valued higher than a citizen's right to privacy, then one would possibly assume that it can be justified to allow NIA to infringe upon their citizens' privacy. This would be in line with the arguments of the NSA, shown in section 4.2.1.

In addition, Hanna (2018) and moderate deontologists such as Judith Thomson held that a right in fact can be infringed if it would benefit the individual and that, in such case, a paternalistic intervention could be applicable. They suggested that rights have *thresholds* beyond which they can be permissibly infringed. This would entail that a citizen's right to privacy can be infringed upon *if* it would benefit the citizen. If then, BDST technologies would benefit the citizen by ensuring national security, then one would be able to claim that it can be justified to allow NIA to infringe upon their citizens' privacy.

Nonetheless, in line with Tännsjö's (2000) understanding of the rights-based ethics, this strand argues that citizens first and foremost have an absolute right to autonomy, which itself entails non-interference in citizens' decision-making (it refutes paternalistic intervention). This implies that the NSA cannot act on behalf of the American population, only by referring to their citizens' welfare. The citizens need to be aware of the NSA's actions, the NSA need warrants for their action and the citizens need to agree to the interference in their decision-making. According to Tännsjö's (2000) interpretation of the rights-based ethics, a state cannot prevent its citizens from taking certain decisions, even if the state would know what the better options for the citizens' welfare are, including a state's end of deterring terrorism.

Consequentialism means that the end can justify the means, but the conclusion that can be drawn by consequentialism is ultimately dependent on what end we maintain is particularly crucial to emphasise. It would in this case either be 1) the consequences of surveillance for national security, 2) the consequences of Snowden's leakages for national security or 3) the consequences of surveillance on privacy. Furthermore, it would depend on the value-hierarchy, as either national security or citizens' privacy is valued higher than the other.

Regarding the consequences of surveillance for national security, the NSA (n.d.) meant that the bulk phone records collection through section 215 could have hindered 9/11 from occurring and that the section was crucial in apprehending Zazi in 2009. Erwin (2014), however, meant that section 215 neither would have helped to hinder the 9/11 plot nor was essential in apprehending Zazi. It cannot therefore be claimed that there was *no other available option* (see section 2.2) than using section 215 that would better ensure the end national security. Therefore, the NSA's act to use section 215 cannot be regarded as rightful.

Erwin (2014) explained that the e-mails that were intercepted by the NSA through section 702 and PRISM gathered sufficient information for capturing Zazi. The NSA (n.d.) also argued that the arrest of Zazi was made possible through the mass-collection of intelligence information, which in turn was thanks to section 702. Even though one cannot rule out that there was no other available option that would provide better consequences, PRISM helped ensure the end national security *better than* the other technologies and means. Therefore, the act of the NSA to use PRISM can be regarded as rightful and thus allowed, but not necessarily as an act that *should* have been performed.

Concerning the consequences of Snowden's leakages for national security, Ledgett stated that Snowden's actions put peoples' lives and national security at risk. It was earlier concluded in section 4.2.2 based on the arguments of the NSA, that without the usage of BDST, the NSA are not able to uncover potential national security threats and that Snowden's disclosures has resulted in a decreased ability to have insight into the actions of terrorists.

Regarding the consequences of surveillance on privacy, Strauß (2018) explained that XKeyscore represented an example of infringement on privacy. Additionally, TrapWire infringed upon citizens' privacy as it was monitoring citizens' movements through surveillance cameras. NSA held, however, that it could predict terrorist attacks. If the end is to ensure

citizens' right to privacy, then it cannot be claimed that there was *no other available option* than using XKeyscore and TrapWire which would provide better consequences.

The NSA acted paternalistically by taking decisions on behalf of the American citizens without the citizens being aware of this, referring to their citizens' welfare. In line with consequentialism, the NSA used BDST as a means towards their end of ensuring national security. One cannot for certain assert that there was *no other available option* that would provide better consequences. If the NSA had taken decisions on behalf of the American citizens with them being *aware* of it, the NSA might not have been able to implement BDST technologies in order to ensure the end of national security. Having in mind that Snowden's public revelations put national security at risk. Therefore, the NSA's paternalistic act cannot be deemed as non-rightful if it would benefit the citizen by ensuring national security. The act cannot be deemed as rightful neither, as XKeyscore and TrapWire infringed upon citizens' privacy and therefore cannot be used as a means towards the end of ensuring citizens' privacy.

6. Conclusions

- *Can it be justified to allow national intelligence agencies to infringe upon their citizens' privacy through big data surveillance technologies in order to ensure national security?*

Given that our point of departure is the duty-ethical strand of deontology, it cannot be justified, as it would treat the citizens *exclusively* as means towards an end.

Given that our point of departure is the rights-based strand of deontology and that we perceive it in the same manner as Tännsjö, it cannot be justified. Nonetheless, if we perceive the rights-based strand according to Hanna and to moderate deontologists, it can be justified, assuming that the BDST technologies would benefit the citizen, even if it would infringe upon the citizen's right to privacy. That these would de facto benefit the citizen is dependent on whether one values citizen's right to privacy or a state's right to self-defence higher.

Given that our point of departure is consequentialism and that the end national security is valued higher than the end of ensuring citizens' privacy, it can be justified, as the act of NSA to use FISA section 702 and the BDST technology PRISM ensured national security. However, it cannot be justified if NIA use section 215 of the U.S. Patriot Act and bulk phone records collection, as it did not ensure national security. Given that the end of ensuring citizens' privacy is valued higher than national security, it cannot be justified as using the BDSTs XKeyscore and TrapWire infringe upon citizens' privacy.

Given that our point of departure is both paternalism and the utilitarian strand of consequentialism, it cannot be justified as the NSA's paternalistic act cannot be deemed as exclusively rightful.

7. Future Research

Potential future research could involve in-depth studies on the Snowden case with the application of the normative logics *contractualism* or *appropriateness ethics*. It might be interesting to consider the agreements or contracts between the state and its citizens, concerning state power vis-à-vis privacy rights, through *contractualism*. One could also conduct an analysis of the pre-9/11 circumstances, to discover what de facto led the NSA to conduct digital surveillance, through *appropriateness ethics.* One other alternative may be to dive deeper into either the actions of Snowden or the NSA, to fully grasp the complexity of the ethical dilemma. Furthermore, one could apply the *critique of ideas* method to potentially find obscurities, inaccuracies, and contradictions with both the arguments of Snowden and the NSA.

8. References

Badersten, Björn. 2006. *Normativ metod: Att studera det önskvärda.* Lund: Studentlitteratur AB.

Beckman, Ludvig. 2005. *Grundbok i idéanalys: Det kritiska studiet av politiska texter och idéer.* Stockholm: Santérus Förlag.

Beckman, Ludvig. 2006. Idékritik och statsvetenskapens nytta. *Statsvetenskaplig Tidskrift* 108(4): 331–342.

Bellaby, Ross. Going dark: anonymising technology in cyberspace. *Ethics and Information Technology* 20: 189–204. https://doi.org/10.1007/s10676-018-9458-4

Buchanan, Allen. 1978. Medical Paternalism. *Philosophy & Public Affairs* 7(4): 370–390. http://www.jstor.org/stable/2264963

Cambridge Dictionary. N.d. *Infringe upon*. Available at: https://dictionary.cambridge.org/dictionary/english/infringe-on-upon (Accessed: 29-11-22).

Dworkin, Gerald. 1972. Paternalism. *The Monist* 56(1): 64–84.

Dworkin, Gerald. 1988. *Theory and Practice of Autonomy*. Cambridge: Cambridge University Press.

Erwin, Marshall. 2014. *Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection.* Available at: https://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Leahy.pdf (Accessed: 2022-12-04).

Gert, Bernard. & Culver, Charles. 1976. Paternalistic Behavior, Philos. *Public Affairs*, 6(1): 45-57.

Hanna, Jason. 2018. Paternalism and Moderate Deontology. In Hanna, Jason. 2018. In *In Our Best Interest: A Defense of Paternalism.* Oxford: Oxford University Press. 118-144.

Hays, Demelza. 2015. *The Ethics of Government Surveillance: Is Edward J. Snowden a Hero or a Villain?* Liechtenstein: University of Liechtenstein.

Just Security. N.d. Marshall Erwin. Available at: https://www.justsecurity.org/author/erwinmarshall/ (Accessed: 2022-12-17).

Mazzetti, Mark. & Sanger, David. 2014. Top Intelligence Official Assails Snowden and Seeks Return of N.S.A. Documents. *The New York Times.* 30 January.

https://www.nytimes.com/2014/01/30/us/politics/intelligence-chief-condemns-snowden-and-demands-return-of-data.html (Accessed: 2022-12-02).

Merriam-Webster. (n.d.). Privacy. Available at: https://www.merriam-webster.com/dictionary/privacy (Accessed: 29-11-22).

National Security Agency – NSA. (n.d.). Available at: https://www.nsa.gov/Signals-Intelligence/FISA/ (Accessed: 29-11-23).

National Security Agency – NSA. 2014. Remarks by Mr. Richard H. Ledgett, Jr., Deputy Director, National Security Agency, at TED Talks 2014 Conference. In Ledgett, Richard. 2014. *The NSA responds to Edward Snowden's TED Talk*. [online]. TED talks. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618716/remarks-by-mr-richard-h-ledgett-jr-deputy-director-national-security-agency-at/ (Accessed: 22-12-07).

Orwell, George. 1949. *1984.* London: Secker and Warburg.

Osisanya, Segun. N.d. National Security versus Global Security. *The UN Chronicle*. Available at:https://www.un.org/en/chronicle/article/national-security-versus-global-security (Accessed: 22-11-29).

Sætnan, Ann. Schneider, Ingrid. & Green, Nicola. 2018. The Politics of Big Data: principles, policies, practices. In Sætnan, Ann. Schneider, Ingrid. and Green, Nicola. (eds.). 2018. *The Politics of Big Data: Big Data, big brother?* London: Routledge, 1- 18.

Snowden, Edward. 2020. *Permanent Record*. London: Pan Macmillan.

Strauß, Stefan. 2018. Big Data – within the tides of securitisation? In Sætnan, Ann Rudinow. Schneider, Ingrid. and Green, Nicola. (eds.). 2018. *The Politics of Big Data: Big Data, big brother?* London: Routledge, 46-67.

The United Nations Office of the High Commissioner for Human Rights (OHCHR). 2013. *The right to privacy in the digital age.* https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age (Accessed 2022-10-30).

The United Nations Office of the High Commissioner for Human Rights (OHCHR). 2022. *Spyware and surveillance: Threats to privacy and human rights growing, UN report warns.* https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report (Accessed 2022-11-02).

Tøndel, Gunhild. & Sætnan, Ann Rudinow. 2018. Fading dots, disappearing lines – surveillance and Big Data in news media after the Snowden revelations. In Sætnan, Ann Rudinow. Schneider, Ingrid. and Green, Nicola. (eds.). 2018. *The Politics of Big Data: Big Data, big brother?* London: Routledge, 197-224.

Tännsjö, Torbjörn. 2000. *Grundbok i Normativ Etik.* Stockholm: Thales.

Ünver, Hamid. 2018. Politics of Digital Surveillance, National Security and Privacy. *EDAM: Cyber Governance and Digital Democracy.* Available at: *https://edam.org.tr/wp-content/uploads/2018/04/Chrest_Surveillance2.pdf* (Accessed 2022-12-28).

Yael, Onn. 2005. The Right to Privacy – The Theoretical Basis. In Yael, Onn et al. (eds.). 2005. *Privacy in the Digital Environment.* Haifa: Haifa Center of Law and Technology, 1-20.