Avoiding Panopticon

Reconsidering privacy violations by governments

MSc Thesis – Final Version

Alex Klein
S0517585
Advisor: Dr. P. Nieuwenburg
Second reader: Dr. M.A. de Geus

Date: June 11th, 2012
Wordcount: 19.018

TABLE OF CONTENTS

I. INTRODUCTION

Jeremy Bentham, the famous British philosopher who is often credited as the founding father of utilitarianism, dedicated much of his life to the realization of a Panopticon. This was a prison where, through the use of mirrors, inmates could be observed all the time without them being able to tell whether they were being watched or not. Because they were unaware of whether the gaoler was watching them or not, the prisoners would always behave properly. (Semple, 1993, p. 20-41) Embittered by years of failed struggle to start an experimental Panopticon, Bentham abandoned the project with the following words: “I have sown the seed; but the harvest I fear, is for another age.” (Semple, 1993, p. 38)

Bentham appears to have been right about the harvest coming in another age. Slowly but surely, governments of Western countries are building their own Panopticons. The subjects are not criminals, but all citizens. And the citizens are not in prison, but in their own homes and on their own streets. Technological progress allows governments to collect more and more information about us. Where we are at any given time, how often we travel to a certain place, and what things are of interest to us. Even fifteen years ago, Richard Spinello wrote about “the end of privacy”. (Spinello, 1997)

Although I am not as cynical of the state of our privacy as Spinello, and I do not think we are actually living in a modern day Panopticon, government is learning more and more about us, thereby reducing the privacy that we have. And just like the inmates in Bentham’s prison, we might one day find ourselves in a situation where we feel like we have to behave exactly like our goalers desire.

In reality things are not that bad, and everyone can enjoy some amount of privacy in their lives. Yet we can see that the government is increasing its efforts to monitor how we behave: through security cameras, phone taps and by analyzing our e-mails. We are often told that it is in our best interest: that we have to sacrifice some of our privacy so the government can do a better job at preventing criminals from harming us and stealing from us.

One might say that security, which is the protection of individuals against violence, crime and terrorism, is the most important task of any government. This idea is confirmed by a strong tradition in political theory: for Thomas Hobbes, the only reason that we established states is to protect ourselves from each other. By giving power to an absolute authority (the

Leviathan), we exchange all our liberty for security. However, in a lot of cases an increase of security is only possible when it is combined with a decrease of liberty, which we also value.

In political theory, the clash between liberty and security is a classic one. Several authors have tried to find a balance between the two, with very different conclusions. In the case of privacy, the clash between liberty and security is important because privacy is a form of liberty, and the privacy of individuals is usually restricted to increase security. It seems to me that privacy is something that should be valued, and that individuals have a right to privacy. Therefore, a decrease of privacy is always undesirable. However, a decrease of privacy might be excusable if there are enough positive consequences for our security. This means that there are certain necessary conditions that should be fulfilled before we can call a decrease of privacy of individuals justifiable. The main task of this thesis will be to investigate what these conditions are. So my main research question will be:

Which conditions should be fulfilled for governments to be justified to restrict the privacy of individuals?

To answer this question, several underlying questions have to be answered. First and foremost, privacy and security are abstract concepts, and should be carefully defined before I can start discussing them. Hence, my first sub-question will be:

How should we define privacy and security?

I think everyone will agree that privacy and security are essential to human beings. We might even say that we have a right to both privacy and security. If this is the case, it will certainly be important for the answer to my main research question. So my second sub-question is:

To what extent do we have a right to privacy and a right to security?

Simply determining that we have these rights isn't enough, of course. In a lot of situations, these rights will clash and upholding one will have to take precedence over upholding the other. So to continue our discussion, I have to analyse how the right to privacy and the right to security relate to each other. My third sub-question will be:

How should we act when privacy and security conflict?

When privacy and security are in conflict, a key issue is in whose interest they are. Those whose privacy is restricted are not always the ones who benefit from the alleged increase in security, and vice versa. So I will take a good look at this, and then answer my fourth sub-question:

Whose interests are playing a role in conflicts between privacy and security?

In the final chapter of this thesis I will answer my main research question and provide some suggestions for future research.

II. DEFINING PRIVACY AND SECURITY

Before we can start comparing the importance of privacy and security we should first determine what precisely is meant by those terms. Especially privacy is a highly volatile and elusive concept, and political philosophers disagree about what it exactly is and whether it even exists. Security is a somewhat less complicated concept, but to avoid confusion along the way I will also clarify what it means.

In this chapter I will define privacy and security, and I will address two problems that arise when we want to "measure" how much privacy an individual has.

1) What is privacy?

Many authors have attempted to define privacy. In this chapter, I will discuss some relevant concepts of privacy. However, before I start defining privacy, I will first deal with the most serious critique of privacy: reductionism. (DeCew, 2002) The idea of reductionism is that there is no such thing as privacy. Whenever someone is talking about privacy, he is actually talking about some other right that he believes to be important. The most well-known reductionist theory is that of Judith Thomson, who gives the example of a man who owns a pornographic picture and keeps it hidden in a safe. Breaking into the safe and looking at the picture would certainly be a violation of privacy. According to Thomson, this claim on a violation of privacy is derived from other rights: rights that come from the possession of the picture. (Thomson, 1975, p.299) Privacy is therefore reducible: every part of privacy can be derived from another right. This reduces privacy to nothing more than a 'front', an umbrella right that is only based on other rights. Talking about privacy and basing legislation on its apparent violation is only confusing: according to Thomson we should simply talk about the underlying rights.

I would argue that there are three ways to refute this argument. First of all, Thomson can only sustain her theory by assuming that a different right is violated. In the case of the pornographic picture, she states that the violation is a violation of property, because individuals have a right not to have their property looked at. However, as Thomas Scanlon persuasively argues, if I borrowed it from a friend and I use it with his permission, my privacy is still violated, even though the picture is not mine and I therefore have no possession rights. (Scanlon, 1975, p.318) This shows that a violation of privacy can occur without any underlying rights being violated.

A second argument is about the reducibility of principles. William Parent argues that

Thomson tries to base her argument on the existence of a lot of rights, some of which are quite difficult to prove. (Parent, 1983, p.279) The right not to be looked at, for example, is questionable at best. If we were to dissect such a right, we might find the same underlying principles as for privacy. This suggests that the reductionist theory makes analyzing and discussing rights unnecessarily complicated.

Finally, even if Thomson is right, and privacy is merely an umbrella term for a cluster of other rights, the concept of privacy still has merit in discussions about policy. For example, when we are arguing about installing more cameras on street corners so the police are more successful in fighting crime, it is much easier to talk about the umbrella concept of privacy than discussing all of the rights that would have to be discussed in a reductionist discussion that tries to avoid using the word ‘privacy’. Most rights are related: autonomy is closely related to liberty, bodily integrity is closely linked to human dignity, and so on. There are no irreducible, ultimate values, and we don't have to refrain from using privacy as a useful concept because of it.

What then is privacy? I would argue that privacy is a condition that we can ascribe to human beings. Just like we can call 'being red' a property of a red sweater, we can call 'having privacy' a property of a human being. And just like there are a lot of different shades of red, there are a lot different states a person’s privacy can be in. I can be in a state of perfect privacy, in a state of no privacy, and somewhere in between. It is not hard to find examples of these different states: a hermit living all by himself in a small house in the woods, with nobody knowing that he lives there and nobody even being aware of his existence, can be said to be in a state of perfect privacy. A person who is displayed on a platform at a crowded square, completely naked, with all his personal information displayed on a large television screen for everyone to see, can be said to have almost no privacy.

Of course, almost nobody in the world is in one of these extreme situations. We are all somewhere in between these two. Some of us are more like the hermit, and others are more like the naked man on the platform. This shows that privacy is not a dichotomous property, but is a matter of degree. In this sense, privacy is akin to concepts like liberty and autonomy.

Even though everyone will agree that the hermit has a lot of privacy while the publicly exposed naked man doesn’t, we still have not discussed what privacy actually is. If we want to know how certain policies can influence the privacy that individuals have, we must determine what privacy is and how we can actually measure it.

There are several definitions of privacy in philosophical literature. I will deal with the two that are most prominent. The first one is defended by (among others) Parent, who argues that privacy can be defined as the control over information about oneself. The second one is defended by (among others) Ruth Gavison, who argues that privacy can be defined as the control over access to oneself (where access also includes information). I will argue that both definitions are correct to some extent, but they are also wrong on certain points.

Privacy as the control over information about oneself is a concept that is defended by Parent. He gives the following definition of privacy: “Privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him.” (Parent, 1983, p. 269) He also argues that, when it comes to privacy, 'knowledge' can only be understood as facts, since falsehoods are already condemnable as libel or slander.

There are two elements in this approach to privacy that are wrong. The first element is the statement that there is only a decrease of privacy when the published information was previously undocumented: “What [already] belongs to the public domain cannot without glaring paradox be called private; consequently it should not be incorporated within our concept of privacy.” (Parent, 1983, p.271) The problem with this statement however, is that it does not appreciate the significance of the accessibility of certain publications. If I find a piece of private information about a famous politician in a fifty year old newspaper article that is currently unknown to the wide public, there is certainly a decrease of the politician’s privacy when I give the information to a journalist who publishes it in the New York Times. The more accessible the private information is, the less privacy a person has. (DeCew, 1997, p.30)

In the same way there is a difference between only one or two friends knowing about my sexual preferences, or the entire country knowing it. In both cases the information may have been documented (for example, in the diary of one of my friends in the former case and in a recent national newspaper in the latter), but this does not change the vast difference between the first privacy violation and the second. But whether it has been documented before or not is relevant for the amount of privacy that the subject loses. If I tell a friend about the story I have read in a prominent national newspaper about a celebrity’s drug use, and millions of readers already know about the drug use, there is less of a privacy violation than if I told my friend the story if it wouldn’t have been in the papers. So accessibility is relevant, but it can be argued that Parent is wrong because he believes private information can be in only one

of two states: documented and undocumented. There is a vast grey area between those two states, because of the role of accessibility.

A second problem with Parent's theory is his statement that there is only a decrease of privacy when the information is true. The problem with this view is that when certain private information is published about someone, this person can be forced into a position where he has to involuntarily release private information in order to disprove the previously spread falsehoods. Consider the following example of a politician who is not having an affair. The public does not know anything about the politician's love life, and the politician intends to keep it that way because he believes his love life is private. When a journalist publishes an article claiming the politician is actually having an affair, the politician might feel forced to prove that the story is wrong in order to rectify the falsehood that has been spread. So even though no true information is released by the journalist, the privacy of the politician has been indirectly diminished.

Gavison defines privacy in a different way. "Our interest in privacy [...] is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and to the extent to which we are the subject of others' attention." (Gavison, 1980, p.423) She believes that privacy exists of three independent and irreducible parts: secrecy, anonymity, and solitude. (Gavison, 1980, p.434) When an individual is completely inaccessible to anyone else, he enjoys perfect privacy (and therefore also perfect secrecy, perfect anonymity and perfect solitude). However, the problem with Gavison's definition is that although 'physical access' and 'attention' may look like being different from the 'information' aspect, I think they are essentially the same elements, which makes her theory of privacy as control over access nothing more than a theory of privacy as control over information.

Gavison argues that physical access is distinct from knowledge, which is true. Yet if we look at it closely, we can see that it doesn't differ that much from knowledge. It seems to me that 'physical access' consists of two different sorts of access. If there would be any physical contact, I don't see that as a decrease of privacy, but as a violation of bodily integrity. When someone who is both blind and deaf hits another person, he will obtain no information about the person. But he will violate a right to bodily integrity and definitely has physical access, yet he does not decrease the amount of privacy the subject has. On the other hand, when there is no physical contact but merely proximity, what would be objectionable to physical access? Physical proximity simply makes it easier to obtain information about

someone else. If our blind and deaf person would be quietly sitting next to you on a park bench, would that be a decrease of your privacy? I don't think it is. Although he has physical access to you (expressed as proximity), the simple fact that he won't be able to observe you (so he can't obtain any information) guarantees that he does not decrease your privacy.

The second element that Gavison distinguishes from knowledge is attention. She uses the example of the president walking the streets incognito. If one were to shout "Here is the president", the president would lose his anonymity and everyone would give him attention. (Gavison, 1980, p.432) This is not in any way different from obtaining knowledge. One obtains information by paying attention to someone. In the example of the incognito president, revealing his identity would give persons all kinds of information about the president, such as shops that he had just visited, or the piece of information that the president apparently likes to walk on the streets in disguise. The reason that someone wants to remain anonymous is that he does not want anyone to get information about him. Thus, attention is not different from knowledge.

Another explanation could be that the president wants to be left alone while walking the streets. He may be tired of being recognized everywhere he goes and may want to experience street life without security guards that are protecting him, cameras filming him and citizens wanting to shake his hand. This line of thought is following the definition of privacy that was introduced by Supreme Court Justices Samuel Warren and Louis Brandeis: "the right to be let alone". (Warren & Brandeis, 1890, p. 193) What if the president does not care about people knowing that he likes to walk on the streets in disguise, but only wants to keep crowds from gathering while he is shopping for groceries? If that is the case, he is not fearing the loss of privacy itself, but the consequences of the privacy loss. Crowds will only gather once they have obtained the information that the president is walking in their near vicinity. Consequently 'being let alone' is a result of having privacy, not privacy itself.

To conclude this part of the chapter, I would argue that we can define privacy as the condition in which information about oneself is not known by others. The amount of privacy that an individual has can therefore be completely measured by how much information about him is known by others. In addition, the more accessible this information is to others, the less privacy the individual has. Accessibility here can be understood both in terms of active accessibility (the ability to find the information if you are specifically looking for it) and passive accessibility (when you can be confronted with the information when you are not specifically looking for it, for example when it is in the headlines of a national newspaper).

2) Two problems with measuring privacy

In the beginning of this chapter I called privacy "a volatile and elusive concept." I did this because I believe that it is hard to measure privacy. With measuring I do not mean that we actually have to be able to quantify how much privacy I have and how much privacy my neighbor has, but we should be able to tell when someone's privacy has decreased. Surely, this is hard to do, because privacy is a highly subjective concept. If we want a concept like privacy to have weight in certain decisions about policy, we should be able to deal with the subjectivity of privacy. I believe there are two reasons for this subjectivity, and I will discuss both.

The first reason is related to the example I gave earlier in this chapter: about privacy being a property of a human being like a red color being a property of a sweater. This comparison is true in the sense that both 'privacy' and 'red' can be used to describe the object or person. However, it is false in the sense that the redness of the sweater is objective, while the privacy of the person is not. We can observe the sweater in a number of ways, and every time the conclusion will be that it is red. Of course, someone might disagree and believe it to be more of a pink sweater, but this is just the subjective interpretation of how we should name the color of the sweater. The color itself does not change, whether someone claims that it is blue or not, because the color of the sweater is independent of what we think of it. It is red in and of itself.

In this sense, privacy is different. Whether a human can be called 'private' is not independent of other persons. Privacy is a relational property, one that is determined through the interaction with others (or the lack thereof). As a result, the amount of privacy that we enjoy can suddenly change. One moment, the hermit in the woods enjoys complete privacy in his small hut, the other moment a large group of tourists accidentally finds him. His privacy is decreased through interaction with other humans, while the redness of the sweater will not change in such a way.

Since privacy is determined through our interactions with other persons, it is hard to objectively measure it. I might believe that I have a lot of privacy when it comes to my political convictions, while someone has been telling other people about what party I usually vote for behind my back. Privacy can be measured as information, but we cannot objectively find out what other people know and whether they possess a piece of private information or not. This also makes privacy harder to measure.

I do not have a definitive solution for the difficulties that arise because of the fact that

privacy is determined through interaction with others. But I do not believe that I have to provide such a solution here. I am merely contending that these difficulties are real, and that they make our discussion about privacy harder.

The second reason that makes privacy volatile and elusive can be found in the words "information about oneself" in my definition of privacy. Any piece of information about me could fall under the definition. The name of my dog, my political views, my sexual preferences, and the color of the sweater I was wearing on May 30th, 2011. It feels strange that even meaningless information such as the color of my sweater should fall under a definition of privacy. If we were to argue, as I will in the next chapter, that privacy should be protected, this will lead to undesirable situations where I can claim that nobody may know anything about me.

If we want to protect privacy, we will have to put some restraints upon the concept op "information about oneself". I will do this in the next chapter, where I shall analyze the right to privacy. For now, I will state that every piece of information about oneself falls under the definition of privacy, even the ones that might seem insignificant. In fact, if we want to measure how much privacy one has as objectively as possible, there is no room for normative decisions about what kind of information is private and what kind of information is not.

So I do believe that if we want to talk about protecting privacy, we should limit "information about oneself" in a way that only information that we actually consider to be private is protected. However, when formulating a descriptive definition of privacy I do not think these limits are necessary, so my definition does not need to be altered.

3) What is security?

Security is a concept that is less controversial than privacy. While there are people who are claiming that privacy is not that significant and that we don't have a right to privacy, almost everyone will agree that individuals should be protected against physical harm. Since it is so broadly accepted I will only very briefly discuss my definition of security.

I would argue that security consists of two components. The first component is the absence of violation to the physical integrity of a human being. This implies that we are not killed, raped, or beaten by other individuals. It is safe to say that almost nobody prefers death over life or being beaten over not being beaten. Protection of our physical integrity is usually viewed as one of the most important (if not, the most important) tasks of any government. For

a lot of philosophers, it even is the only reason that we should have governments at all. For Thomas Hobbes, for example, getting out of the miserable and violent state of nature was the only reason why we would voluntarily restrain ourselves by subjecting ourselves to the authority of a state. (Hobbes, 1651, p. 93)

The second component of security is the protection of property. This would include the government preventing other individuals from stealing property that is rightfully and legally yours. Because a large part of our lives is devoted to accumulating property and possessions, a society where individual property is not secure will be a society in which individuals will not feel secure either. Of course, there is a lot of discussion among scholars about property, and about how much should be rightfully and legally ours. However, I do not wish to engage in a debate about distributive justice here. The possibility to own property is acknowledged in virtually any society, and for that reason we can include it in our definition of security.

Are these two components equally important? I would argue they are not. Physical integrity is more significant than property, something that almost everyone will confirm. Enjoying physical safety without owning property is to be preferred over being a rich man who is beaten up on a regular basis. Also, in the first situation it is easier to start gathering property than it is to gain physical safety in the second. That physical integrity is more important than property is confirmed by a lot of actual discussions about privacy: governments usually justify a measure that reduces privacy by an appeal to physical safety, because most people would rather be the victim of theft than be murdered.

In conclusion, it seems to me that someone enjoys security when he is free from murder, rape, violence, and theft. Not coincidentally, such material phenomena are usually the subject of many government measures that decrease individual privacy, such as camera surveillance. In fact, that is the reason why I have chosen for this specific definition of security. It may not be a perfect definition, but it does provide us with a clear idea what is at stake in the debate about privacy and security.

A crucial difference between security and privacy becomes clear at this point. While privacy is a rather abstract concept, security is more concrete. This is because privacy is expressed through information, while security is much more ‘physical’. It is much easier to observe that someone has been murdered than that someone’s privacy has been violated. As I have shown above, privacy can be hard to measure for different reasons. Security is not troubled by this. If we want to know how secure people are in a certain neighborhood, all we have to do is find the statistics about violence and theft and we know what we are dealing

with. This makes security more ‘tangible’ than privacy for a lot of people, and this is one of the reasons that security is often deemed more important than privacy.

Evidently, there is more to security than physical integrity and property protection. A key psychological element also exists: the belief that someone is secure. We can be as secure as possible, yet still feel threatened because we believe our security is not guaranteed. And vice versa, we can have a strong illusion of safety while there actually is a large chance that we will be killed or robbed. Although individuals may usually have an accurate idea of how much security they enjoy in their own society, in a lot of situations people may overestimate or underestimate threats to their security. Even in a society with almost no crime, people may be afraid because the media pay a lot of attention to the relatively few criminal acts that do happen.

The belief of how secure you are is pivotal in discussions about privacy, because it can be observed that a lot of government measures are simply in place because they give the public an illusion of safety, even though the measures are not contributing to a safer situation at all. As Daniel Solove notes about random searches of people’s baggage on the New York subway, the measure “seems more symbolic than effective, because the odds of the police finding the terrorist with a bomb are so low.” (Solove, 2008, p. 348) However, such symbolic measures may still have value, because they might make people feel more secure.

Why is it important that people feel secure? Apparently this is so because it enhances the freedom that people have. When you fear that you will be killed or robbed every time you walk on the street, you will be less likely to actually walk the streets. And when you believe that there is a very high possibility that someone will break into your house to steal your television set, you are far less likely to feel relaxed and may not even leave the house as much as you’d like to. The psychological consequences of believing you can indeed enjoy society are also considerable. When you believe that your physical safety and property are effectively protected, you will be more likely to start relationships with other individuals and work to accumulate property.

All this is possible even when the feeling of security is actually an illusion. In that sense, ignorance might be bliss. Alternatively, when you are enjoying a high level of security but don’t believe that you actually are secure, this will very probably affect you in a negative way (which is an interesting explanation why governments usually want to fix this incorrect security assessment of society). Obviously, if we would have to prioritize being secure and feeling secure, the former would trump the latter. Generally everyone prefers not being

murdered above feeling safe about not being murdered. The key issue here is that the feeling of security is also relevant in discussions about privacy.

I do not think my definition of security as physical integrity and property protection is the only possible definition. However, I would argue that it is adequate enough for our discussion about privacy and security, because preventing or punishing violence and theft are usually the reasons which governments propose when they want to take measures that reduce privacy.

III. A RIGHT TO PRIVACY AND A RIGHT TO SECURITY

In the previous chapter I have given definitions of privacy and security, and I now turn to both concepts as rights. I will begin with an explanation of what rights are, and will address different categories of rights that can be distinguished. Subsequently, I will argue that we indeed have a right to privacy and have a right to security as well.

1) What are rights?

Before discussing whether we have a right to privacy and security or not, we must first take a closer look at the concept of rights, since noting that I have a right to something raises many questions. Why do I have this right? Should everyone respect it, or just certain agents? Is it an absolute right that may never be violated?

To be sure, there are countless definitions of rights. This is not the place for a discussion about the exact definition, so I will use one that is appropriate for my purposes: "rights are entitlements (not) to perform certain actions, or (not) to be in certain states; or entitlements that others (not) perform certain actions or (not) be in certain states." (Wenar, 2005)

I realize there is a lot more to rights than just this definition. Wenar's definition includes different elements that we might call rights. These elements are based on a well-known categorization of rights by Wesley Hohfeld, who sees four kinds of rights: claims, privileges, powers and immunities. (Hohfeld, 1923, p. 36) Having a privilege means that one is allowed to perform or not perform a certain action. Having a claim means that someone else has an obligation to another person to perform or not perform a certain action. Having a power indicates that I can change my own or someone else's claims or privileges. Finally, having an immunity means that someone else is not allowed to change certain claims or privileges.

In order to add more transparency to this categorization, Hart uses only two categories of rights: primary and secondary rights. With primary rights (claims and privileges) "human beings are required to do or abstain from certain actions, whether they wish it or not." Secondary rights (powers and immunities) "are in a sense parasitic upon or secondary to the first; for they provide that human beings may by doing or saying certain things introduce new rules of the primary type, extinguish or modify old ones, or in various ways determine their incidence or control their operations." (Hart, 1961, p. 78-79)

This distinction between claims, privileges, powers and immunities will become crucial later on in this chapter and in the next one, so I will try to clarify it with an example. Let's say that I have a right to life. In the primary dimension, this suggests that I have a claim against everyone else that they do not end my life. This claim can be against other individuals and against the government. In the primary dimension, I also have an immunity against my neighbor changing this claim. He can not suddenly choose to remove my claim that I am no to be killed. However, a judge for instance may have power over my claim. If I live in a country where the death penalty is allowed, a judge may decide to extinguish my right to life by sentencing me to death. I am not arguing that it is necessarily good that a judge can do this (opponents of the death penalty obviously oppose the judge's power-right over my claim-right to life), yet the judge has the power anyhow.

This raises a new question: where do rights actually come from? Legally speaking, in democratic societies rights are usually granted by parliamentary majorities and embedded in laws. Yet what is the reason for us to create and grant things like rights?

Granting rights is meant to settle disputes of how to act in advance. If I am planning to kill my neighbor because I just don't like him, I might stop to think about my action for a moment. I might weigh the positive and negative consequences for myself and (if I am empathetic) for my neighbor. If I were to decide that the positive consequences for me (getting rid of my annoying neighbor) outweigh the negative consequences for my neighbor (death), I would probably go next door and kill him. However in the act of weighing the pros and cons, rights will enter the balance. If someone were to convince me that everyone (or at least my neighbor) has a right to life, I might reconsider my actions. In general, rights are a guideline of how to act morally, giving weight to certain values that we hold dear, such as life, free speech or privacy.

How do we decide whether we have a moral right to something? There are two major ways to make such a decision. One is consequentialist and is called an instrumental theory of rights; the other one is deontological and is called the status theory of rights. (Wenar, 2005) I would argue that something can be said for both ways, and I will discuss them now.

Consequentialism judges actions solely on the value of their consequences. The most influential consequentialist theory, utilitarianism, sees an action as moral if it increases (or maximizes) overall welfare or happiness for as many persons as possible. Obviously, this seems to be in conflict with the concept of rights: if we see rights as rules that we should

follow when we act, these rules limit the options that we have. One of the options that is restricted because of a particular right might be the one that produces the best consequences. Consequentialism wants to judge every action on the consequences of that specific action, on a case-by-case basis. This, however, leaves no room for rights, that can restrict us to make the choice with the best consequences. Understandably, then, Sumner comes to the conclusion that "consequentialist theories have a reputation for hostility to rights." (Sumner, 1987, p. 164)

How can consequentialism lead to an instrumental theory of rights? Of course, there are a lot of different theories of rights that are based on consequentialism, but what they basically have in common is that they see rights as tools to achieve the best consequences. In *On Liberty*, John Stuart Mill uses this argument to defend the freedom of speech: in different ways, a right to freedom of speech is vital because it is beneficial to all of mankind. (Mill, 1859, p. 76-78) This might create problems for a consequentialist: if a right is conflicting with a non-right positive consequence, and violating the right has slightly better consequences than respecting it, a consequentialist would have to break the right or depart from his consequentialism: both are undesirable actions.

Undoubtedly, the consequentialist approach to rights has merits. The reason that utilitarianism and consequentialism can "feel" so valid is because consequences matter. When we make decisions in real life situations we always tend to consider the consequences. Politicians would surely become unpopular if they would have no eye for the consequences of their policies. It is pretty difficult, for example, to defend an uneven way of distributing wealth because it is just in and of itself, while simultaneously people are dying of hunger. I shall return to this later.

Deontological theories judge actions not on their consequences, but on how much value these actions have in and of themselves. This specific judgment is usually based on the Kantian idea that human beings are not merely means to an end but the end itself. Instrumental rights are therefore usually based on something like human dignity. Warren Quinn gives a good definition of this, so I will quote him at length here: "A person is constituted by his body and mind. They are parts or aspects of him. For that very reason, it is fitting that he has primary say over what may be done to them – not because such an arrangement best promotes overall human welfare, but because any arrangement that denied him that say would be a grave indignity. In giving him this authority, morality recognizes his existence as an individual with ends of his own – an independent *being*." (Quinn, 1989, p.

209)

I personally prefer status-based rights over instrumental rights, since they offer a more stable system of rights and therefore a more powerful guide on how to act in accordance with these rights. Apart from my personal preference, we should not forget that status-based and instrumental rights are not mutually exclusive. We can defend a right both on basis of the status approach and on basis of the instrumental approach, and if we can do that, the right becomes much stronger. So when we are considering creating a right in our society, the optimal situation would be that it is a right that can be defended from both a consequentialist and a deontological position. A right to life, for example, can be said to both respect and promote human dignity and to have positive consequences for everyone who enjoys the right and society as a whole. I would argue that we can defend both a right to privacy and a right to security in this way, which I will turn to right now.

2) Why we have a right to privacy

It seems to me that privacy is important for every human being, and we should have a right to privacy for both deontological and consequential reasons. I will start with the former.

Privacy can be seen as a status-based right. This approach uses an appeal to human dignity to defend privacy, in a similar way that people who defend a right to bodily integrity appeal to it. If we view privacy from this position, we can hold that human dignity is composed of several elements, one of them being privacy. The most famous defender of this approach is Edward Bloustein, who I will quote here at length. “The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.” (Bloustein, 1964, p.1003)

This view looks a lot like the argument Quinn used to defend status-based rights, and what he said about them can also be applied to privacy. This approach to privacy as a right appeals to the individuality and uniqueness of human beings. By accepting that every human being is a unique individual, we grant him a certain right to be different from the mass, to be

an individual with qualities that are his own.

If we were to completely dissect the mind of a human being, and learn of all his hopes, dreams, fears and secrets and make them public, he would lose his dignity because we would not be viewing him as a human being but merely as the sum of his qualities. If he has qualities that deviate from the public norms and are now made public, he will feel shame, and he will feel forced to change his qualities, therefore changing his individuality. So by acknowledging that persons have a mental area where nobody may trespass, we are actually acknowledging that even though the individual may not be perfect, the dignity that he has as a human being allows him to be, to a certain degree, imperfect, and without public scrutiny threatening that imperfection.

From the consequentialist approach, we will look at privacy as an instrumental right. In this sense, a guaranteed right to privacy is desirable because it promotes freedom. Obviously, this is not the place to engage in the debate about whether freedom is good or bad, I will just state that having more freedom is a positive consequence. This is in line with the consequentialist idea that we should be able to choose the actions that have the most positive consequences for ourselves or for society. The more freedom we have, the more options we have. The more options we have, the bigger the chance is that we can choose an option with positive consequences. I would suggest that a guaranteed right to privacy promotes freedom in two ways.

First of all, when privacy is decreased, freedom is decreased as well because someone else (another individual, or the state) gains power over you. For example, when someone obtains a certain piece of sensitive information that you would not want anyone to know, he can use this information by threatening with publication of the information, unless you do as he pleases, which means your freedom is limited.

Another example is that by gaining information about the individual, the relation of power between the individual and the one that obtained the information changes. (Parent, 1983, p.276) When someone else learns of your fear of spiders, he may use spiders to deter your from entering a building he does not want you to enter. For that reason alone, one might want to hide one's fear of spiders from others. This kind of shift in the power relations between two actors becomes especially relevant when large companies violate privacy: they can use private information about you to make you more incline to buy their products, even though you may not have wanted to buy them in the first place. Consequentially, your freedom to choose the product that you might have wanted is reduced.

Secondly, a decrease of privacy can be problematic for those behaving in a way that might not be illegal, but is frowned upon by society. A lot of societies are intolerant of certain lifestyles, and public shame will be brought upon those that live by these lifestyles. For example, in most countries, homosexuality is not illegal, but we can very well understand why homosexuals might want to hide their sexual preferences: because it is not mainstream and still frowned upon by a lot of people. By guaranteeing privacy, we give them the freedom to live their lives as they want to, without being criticized by others. This argument makes it clear why we definitely should protect privacy as a right, and should not let a democratic society decide what is private and what is not on a case-by-case basis. For the majority of the people may not be ashamed of the things that a minority might be deeply ashamed of. When people argue that they do not object to a certain privacy-violating measure by the government because they have nothing to hide, this is due to the fact that how they behave is probably accepted by society. A person who is the perfect model for how society would want someone to be, might possibly not care about privacy at all (and may even want to expose himself as much as possible). However, privacy is not there to protect them; it is to protect those that do things that may not be illegal, but are not accepted by everyone. By creating this possibility we are creating freedom for people with deviating lifestyles.

Gavison names two other positive consequences of privacy that are not necessarily related to freedom: mental health and human relations. Enjoying privacy promotes mental health, since "individuals may become victims of mental illness because of pressures to conform to society's expectations. Strict obedience to all social standards is said inevitably to lead to inhibition, repression, alienation, symptoms of disease, and possible mental breakdown." (Gavison, 1980, p. 448)

Although the evidence that Gavison gives in favor of this argument is rather weak (especially the word "inevitably" would need a lot more proof), we can imagine that a certain barrier between society's standards and one self is desirable to increase mental health. A lack of privacy means that society has more possibilities to check whether an individual is conforming to specific societal standards or not. If society learns that this is not the case, pressure may be applied in order to make the individual conform to the societal standards, which eventually might lead to mental health problems (or at least to unhappiness, I would think).

Gavison's second positive consequence of privacy is the promotion of human relations. She defends this argument by acknowledging that human relations are only possible if we can somehow keep certain pieces of information away from others. In some sense, this

argument might be explained as the possibility to lie (whether by omission or not) or to behave differently in different environments. For example, people behave differently when they are at work than when they are at home. And we can indeed agree that it would not improve our relations at work if our colleagues would know everything that is happening in our homes, where we are in a different environment and behave accordingly. In this sense, privacy enables us to keep different social environments separate. When someone does not enjoy privacy, this separation is gone and people will be less capable of engaging in human relations. (Gavison, 1980, p. 450)

There are also a lot of negative consequences that specifically apply when the government violates the privacy of an individual, and I will shortly discuss four of them here.

Firstly, the government learns a lot more about its citizens than they ever could in the past. Through data mining and data analysis, the government creates profiles of its citizens that can tell a lot about our characters and our behavior. (Solove, 2008, p. 357-358) Generally, we have no opportunity to see our own profiles to check whether they are accurate or not, giving citizens no opportunity to correct possible errors in such profiles. And although it depends on how much we can trust our government, it is always advisable to be on our guard against governments knowing too much about our behavior (or anyone with that much power over us, for that matter).

Secondly, even though we may trust the government as a whole with our information, 'the government' is merely an abstraction. It consists of a lot of public servants, and although we can generally trust them with sensitive information, we should not forget that they are not "wise, self-restrained angels". (Shue, 2005, p. 235)

Thirdly, government is usually run by some of the parties that we have in a democracy, implying that there are some parties that might have access to a lot of sensitive information about all citizens. Through profiling, they can gain a better understanding of how people think and behave, possibly giving them an edge over the other parties in elections.

Finally, the government is storing data until they have a need for it, or until it has been analyzed. As long as it is stored, the information might leak. As we all know, data leaks by governments happen all too often, while failing to protect data containing citizen's private information is also a definite violation of privacy.

I have provided a number of positive consequences that a right to privacy has for

individuals, and I have tried to explain why we have a right to privacy from a deontological point of view. However, if we want to have a right to privacy that is somehow protected in a legal way, there has to be a certain universality to what we should call privacy and what not. Up until now, I have regarded privacy simply as "information about oneself". And although I think this is the correct definition and all the information about oneself falls under the concept of privacy, I do not think it is realistic that all the information about oneself should be protected by a right to privacy. We have to somehow narrow this concept down by answering the following question: which information is private, and which information isn't?

Clearly, it is difficult to answer this question. Overall, what we consider as 'private' is different for every individual. For example, I do not want anyone to know which websites I have visited during the last month. I would surely want to have this list of websites protected by the right to privacy that I have. Contrastingly, someone else may not care about someone else knowing about his internet activity at all, and have other pieces of information that he would prefer to see protected. So it seems that something can be considered to be private when a particular individual himself feels that it is.

Indeed, this brings about all sorts of trouble. In general, rights need to have a certain universality, especially if we are going to embed them in laws. If we would let everyone decide what pieces of private information they would want protected, we would possibly have all kinds of weird obligations. If a friend for some reason would invoke his right to privacy to prevent me from looking at him while he is walking on the street, that just feels awkward. So what people believe to be private is relevant, but we don't want every person to decide individually what kind of information he has a right to privacy for.

Maybe we should let society decide in a democratic way, which is something we do with a lot of issues. We could hold a referendum where voters can decide for a lot of types of information whether they regard them to be private or not. Types of information that are believed to be private by a majority of the people will fall under the right to privacy. Although this sounds fairly reasonable, it does create problems. Some kinds of information that we might want to protect with a right to privacy are not considered as private by most people because they conform to the norms of society. But a right to privacy is not to protect those people, it is to protect those who do not necessarily conform to the norms of society.

For example, let's say that a random Western government would want to register everyone's political views. The majority of people have moderate views that are accepted by society since there is a majority that holds these views. The majority members would not have

a problem with this register, because they don't feel that their right to privacy should include something that, for them, is not embarrassing at all. Of course, the people that have extreme political views might not want these views to be known to anyone else, but they will lose the referendum that decides whether 'having a political view' should fall under the right to privacy. Evidently, people that truly have "nothing to hide" could still understand those that do, and might be empathic to the latter's desire to have protection of embarrassing information. For instance, the rights that minorities have obtained in the last decades show that minorities can expect this sort of empathy. Defining what is private and what not, should occur through democratic debate, and the burden of proof lies with those who believe that a certain piece of information should explicitly not fall under the right to privacy.

In the end, it remains complicated to think of a specific mechanism to decide what sort of information should be considered private and protected under the right to privacy. Making an objective list is hard because of the many differences between societies and because norms and taboos are constantly changing. Yet I think a list of things to be considered private should definitely include those things that a significant minority believes to be private.

At the beginning of this chapter, I discussed the categorization of rights by Hohfeld and Hart, which will now be applied to the right to privacy. It seems to me that we have a right to privacy against other citizens, but of course this thesis is about the right to privacy that an individual has against the government. The right to privacy is a primary claim-right, which implicates that the individual has a claim against the government having certain kinds of private information about this individual. This issue will be discussed in the next chapter, but first I will shortly argue why we actually have a right to security.

3) Why we have a right to security

In the previous chapter it has been explained what security is. We found it consists of physical integrity and property protection, with a feeling of security also being relevant. Similar to the right to privacy, we can defend a right to security both as a status-based right and as an instrumental right. I will not give much attention to defending the right the security in these ways, because a right to security basically has *prima facie* strength and is accepted by virtually everyone. It is also less complex than the right to privacy, which makes accepting it much easier.

A right to security can be defended on a deontological basis in the same way as privacy: human beings own their body and mind, and nobody else may own it. We therefore have a right that others may not violate, because a violation would mean to deny that we are the ones that are the master of our own body and mind. For this reason, violating physical integrity for whatever reason makes our body the means to an end, while human beings should be an end in themselves.

Defending a right to security on a consequentialist basis is relatively easy: we can contend that physically hurting someone does not only cause a lot of pain and grief (which are things a consequentialist, especially a utilitarian one, will want to avoid), but also emotional and psychological damage. For a utilitarian like John Stuart Mill, preventing harm is the most important task of governments. A right to security defends our bodies against violence and therefore prevents harm, making it a desirable right for a consequentialist.

Essentially, property rights are more complex, and sometimes disputed. The philosophical sub-field of distributive justice concerns itself with these rights, and how we should treat them. (Waldron, 2004) However, it is generally accepted that someone can own property, making him the one that can do with the property what he wants within the limits of the law. Obviously, this thesis is not the place to summarize the entire discussion that surrounds property rights, so I will just assume that we can own property and that property rights are a part of a right to security.

While we do have a right to security (being physical integrity and property ownership), we do not have a right to a feeling of security. Of course, once our right to security is respected, we will probably start feeling safe as well. As such, individuals do not have a claim against the government or other individuals that they should feel safe. A feeling of safety comes from individuals themselves, and if someone feels unsafe without any reason, he is the one to blame, and no one else. The reason that I am dealing with this issue is because in discussions about privacy and security, often the argument that people should be able to feel safe is used to defend privacy violating policies.

Let me now turn back to the categorization of rights. The right to security is a primary claim-right against other individuals and the government: a claim that they do not hurt us and do not steal or destroy our private property. Nevertheless, this thesis is specifically about the government protecting us from violence and theft by other individuals. So the government should respect our right to security, but that is not what this thesis is about: it concentrates on

the primary claim-right of security that we have against other individuals.

IV. WHEN PRIVACY AND SECURITY CONFLICT

When privacy and security are compared, authors usually use the metaphor of finding a balance between the two. This suggests that the image that the government is operating a weighing scale that has to be balanced. In this context, let us assume that the weighing scale is in perfect balance, but because of external factors, such as an increased threat of terrorism after September 11, it is suddenly imbalanced. Thus, the metaphor of balance would lead us to the most obvious action: decreasing some of our privacy so we regain some security, by which the scales are in balance again. (Etzioni, 1999, p. 184)

This chapter will address the issue of balance, and whether the above method of rebalancing scales is actually the appropriate way to cope with changing external factors. After some deliberation I will come to the conclusion that using the image of balance is an interesting way of looking at prioritizing rights, but that there are many problems with it, especially if one jumps to conclusions in the way that Amitai Etzioni does in the previous paragraph.

I will start with an elaboration of how we should deal with rights: whether they are absolute, and what happens when they are indeed violated. This will indicate that we probably do have to balance the two rights out against each other. Then I shall give an analysis of how balancing actually works in the work of certain authors, and explore whether there are faults in the methods that have led them to arrive at very different conclusions about reality, even though it seems their methods are practically the same. I will end with an argument of how balancing should function if we truly care for the right to privacy and the right to security.

1) How should we treat rights?

It is one thing to say that someone has a right, but that still does not tell us how we should deal with these rights in everyday situations. People may choose to voluntarily abandon one of their own rights, and conflicts of rights occur all the time. So I will now address these issues by exploring how we should treat rights in certain situations.

Firstly, I am aware that people may voluntarily abandon or ignore their own rights. To have a right to something means that others should respect this right, not that we ourselves are absolutely required to uphold it. This is especially relevant in the case of the right to privacy, I think, because people decide to share private information all the time. This still counts as a

reduction of one's privacy, but there seems to be nothing wrong with it. Notwithstanding, when I decide to tell a secret to a close friend with the specific instruction that he should not tell anyone else, he is violating my right to privacy when he passes the secret on to others.

Secondly, there exists the idea of rights being absolute. This is an idea which is based on Kant, implying that there are rights that may never be violated, no matter how bad the consequences are, and no matter which other claims we may have that would mean the right has to be violated. I do not think this is true, and it also makes no sense. Like I said earlier while discussing deontological ethics, at some point the stakes will just be too high to not violate the right. As Gavison notes: "It does not mean that privacy is the one value we seek to promote, or even the most important among a number of values to which we are committed. This is true for all our values, however. None is protected absolutely, not even those to which a commitment is made in unequivocal terms in the Constitution." (Gavison, 1980, p. 468)

Raise the stakes enough and even a quintessential right will be overruled by other rights or by security rights of others. If we have to kill someone in order to save a thousand others, it may become tempting to violate the right to life of this one particular individual, especially if this individual was someone that we would consider to be "bad" (i.e. a terrorist or criminal).

Additionally, there is the matter of efficiency. If we would suggest, for example, that security always trumps privacy, this could produce undesirable results, and massive privacy right violations. Let us assume we live in a hypothetical Western society that is rather peaceful, and consists without violations of privacy and other liberties occurring too much there is only one murder a year in the entire country. If we would follow the argument that security always trumps privacy, we should turn this peaceful society into a police state in order to also prevent this one murder a year. This is way too rigorous. Most people will agree that one dead person a year is an acceptable price to pay for liberty for the entire country.

Thirdly, what should we do when a right is indeed violated? I have just argued that rights are not absolute, which means they are sometimes justifiably violated in order to promote a certain good or other right. When we make the consideration that right A (of any given person) outweighs right B (of the same or another person), one will have to violate right B. To be sure, that does not mean that the owner of right B has lost his right. The right is still there, even though it has been violated. Judith Thomson suggests that the term "violated" should be replaced by "defeated", indicating that the right still exists but has been overruled in

this particular case (which also means that in the future, in a different case, right B might defeat another right C). When a right is defeated, Thomson continues, it leaves behind a "moral residue", which means that the person that violated the right has obligations towards the owner of the right. For instance, we could think of an apology, or some way to compensate the damage that has been done. (Thomson, 1990, p. 84-86) This makes sense. The government also does this when it has wrongfully imprisoned someone: these persons usually get a sum of money as compensation, or at the very least an apology. Michael Walzer has phrased this argument in a rather effective way: "When rules are overridden, we do not talk or act as if they had been set aside, canceled or annulled. They still stand and have this much effect at least: that we know we have done something wrong even if what we have done was also the best thing to do on the whole in the circumstances." (Walzer, 1973, p. 171) In the case of privacy violation by the government in order to increase security, this solution seems highly impractical. The government would have to apologize or pay money to everyone to compensate for the privacy violations, since nowadays almost everyone is being filmed by security cameras every now and then. I think that all the good things that our government does for us may compensate this, but we should not forget about the moral residue, and we definitely should not overlook that a right has been violated.

2) Should we balance privacy and security?

If we accept that absolute rights do not exist and privacy and security are not trump rights that always defeat the other one, we must also accept that we sometimes have to violate one right in order to promote the other. Eventually, it seems like we will have to find some way to balance privacy and security.

Such ways have been suggested before. There are many examples of practical frameworks that can be applied to privacy-related legislation to determine whether a violation of the right to privacy is acceptable, and I shall discuss two prominent ones in the next part of this chapter.

Let me start with the image of balance. This image depicts the idea that two "things" are at odds with each other and we have to find an acceptable middle ground in which there is an acceptable amount of both "things" present. In this case, as Jeremy Waldron correctly describes, it concerns finding a balance between an individual's privacy and society's need for protection against harm. In fact, Waldron believes this has the following consequence: "There is always a balance to be struck. And that balance is bound to change (and it is appropriate that it should change) as the threat to security becomes graver or more imminent." (Waldron,

2003, p. 192)

Waldron formulates criticism of the image of balancing privacy and security, but most of it is about how the process of balancing is occurring instead of about the concept of balancing itself. I will return to Waldron's critique on balance later in this chapter, and will give two objections that I have against the image of balance.

First of all, the image of balance gives us the idea that there are two relevant concepts (in this case, a right to privacy and a right to security) that should be weighed against each other. This does not mean that they are the same, or have the same weight, but merely that they can be compared. Just like we can compare the weight of an apple with the weight of pocket watch, we can also compare a right to privacy and a right to security. In principle, the image of balance suggests that they are comparable to each other, while this may not necessarily be the case. Although they are both rights, they seem to be too different to be weighed against each other. The image of balance suggests a certain equality between the two rights that can be doubted. I will come back to this issue later in this chapter, but for now it is sufficient to note that the image of balance suggests that privacy and security are mutually comparable and lie on the same scale, which I believe they are not.

Secondly, based on plausible objections by Lucia Zedner, balancing is often presented as a zero-sum game, "in which more of one necessarily means less of the other." (Zedner, 2005, p. 511) Actually, this is not necessarily the case. Before our governments had advanced methods of surveillance they were also capable of granting us a certain amount of security without invading our privacy as much as they do now. And it is not hard to think of a government policy that has reduced our privacy without increasing our security. Though in a lot of cases it may be true that more of one does mean less of the other, it is not an absolute necessity, something that the image of balance suggests. Our priority should not lie with finding a situation where we have an acceptable amount of privacy and security, but where we have an *optimal* amount of privacy and security.

The semantics of balance are relevant here because, as Waldron noted correctly, balance seems to imply that we have to rebalance once things change, which is certainly not always true. So let me propose a term that does not have these implications: the desirable situation in a society is a privacy-security equilibrium. Now I shall turn to what such a situation should look like.

3) How can we find the privacy-security equilibrium?

Several authors have given frameworks for balancing privacy and security. I will discuss two important frameworks: one by Alan Westin, who argues for more privacy, and one by Amitai Etzioni, who argues for less privacy. The interesting issue here is that their frameworks have a lot in common but they reach very different conclusions about how the status quo should be changed (which can only partially be explained by the gap of 32 years between their books). I will first discuss both frameworks and argue that both of them lack an essential element, and I will conclude this part of the chapter by explaining how we should reach an acceptable privacy-security equilibrium.

Westin presents five steps that we should follow when balancing, so privacy can "receive its proper weight on the scales in any process of balancing competing values":

1. Measuring the seriousness of the need to conduct surveillance.
2. Deciding whether there are alternative methods.
3. Deciding the reliability of the instrument.
4. Determining whether consent to surveillance has been given.
5. Measuring the capacity for limitation and control of the surveillance if it is allowed.

According to Westin, if there is a serious need, there are no alternative methods, the privacy-violating instrument is reliable, there is consent, and the instrument can be controlled, surveillance is allowed. (Westin, 1967, p. 370-377) I would argue that 1, 2, 3 and 5 are all valid steps, and that they should definitely be applied when the government is proposing a policy that might possibly violate privacy. However, they are also quite obvious steps. If there is no serious need (step 1) privacy obviously does not have to be violated to fight a threat (although this seems happens often enough).

Westin's fourth step, about consent to privacy violation, is interesting though. The issue about privacy violation is that it cannot rely on consent. When people can individually choose whether they do or do not wish to be the subject of a policy that violates privacy, those who the policy is meant for (the people that are planning on breaking the law) will usually not give their consent, along with a lot of people who won't break the law but don't want to be observed. This means that the ones that have to be observed in order to increase security are exactly the ones who probably will not want to be observed. To be sure, we could get consent through democratic procedures like we usually do, but that still will not work. If we would let citizens vote in a referendum to decide whether a certain policy that violates privacy should be passed, a majority will most probably vote in favor of it. The reason is that it is usually a

minority that does have something to hide, even though that 'something' is not illegal, but merely something to be more or less ashamed of. So step 4 seems a bit off, but the other steps are all necessary requirements before we are allowed to implement a policy that violates privacy.

Communitarian philosopher Etzioni has a comparable framework of four rules that we should follow if we want to violate privacy of individuals:

1. There should be a well-documented and macroscopic threat.
2. If possible, the government should first resort to measures that do not violate privacy.
3. The privacy-restricting measures should be as minimally intrusive as possible.
4. Undesirable side effects should be treated.

Through this framework, he reaches the conclusion that in a lot of cases, there is too much concern for privacy and not enough concern for the public good (usually something security-related). (Etzioni, 1999, p. 10-15) Personally, I tend to agree with these rules, but just like with Westin's steps, these four rules are basically quite obvious. These sets of steps and rules don't tell us how we should treat privacy and security when they are at odds, neither do they provide us with any reliable tools by which to come to an equilibrium. That explains why both authors come to very different conclusions about the desirability of something like camera surveillance, even though their general frameworks are comparable and not mutually exclusive.

Then how should we do it? Terms like 'balance' and 'equilibrium' suggest that we can have some sort of quantitative analysis of privacy and security. It suggests that when the government is planning to place surveillance cameras with microphones in a crowded shopping street, we can calculate that society will gain 20 points of security but lose 25 points of privacy. This is unrealistic, because we cannot quantify abstract concepts like privacy and security. And even if we could, it would probably be of no use: when the government is considering measures that violate privacy they are always dealing with hypotheticals. We cannot know for sure if the measure will indeed reduce violence. Surveillance cameras may work as a deterrent for criminals, who may decide to not commit a crime at all. However, it may also lead them to simply commit their crime in another area, where there is no electronic surveillance. And, in extreme cases such as terrorism, surveillance cameras will most likely do nothing to prevent a suicide bombing anyway.

For the sake of the argument, let us now assume that we can quantify privacy and

security, and let's assume we can know the consequences for both if a certain government policy is successfully implemented. Even in this case, frameworks such as those of Westin and Etzioni will not give us the answers we are looking for. For instance, there is a certain street in a particular city in a certain Western democracy where there is a moderate amount of crime. The government is facing three options: placing surveillance cameras (policy A), placing surveillance cameras with microphones (policy B) or doing nothing (policy C). Some very smart government employees have quantified the expected consequences to privacy and security for society, and have come up with the following figure:

	Policy A	*Policy B*	*Policy C*
Privacy	*95*	*90*	*100*
Security	*110*	*115*	*100*

So, which option should be chosen? If we value privacy most, we would choose Policy C. If we value security most, we would go for Policy B. And if we are neutral towards the two, we would prefer Policy A, which gives the highest combined amount of privacy and security. The crucial question is, then: which one do we have to choose? Eventually, Westin, Etzioni and other 'balance promoters' do not provide us with an acceptable answer to this question. In the final two sections of this chapter, I will make an attempt to truly compare privacy and security.

4) How do we truly compare privacy and security?

There are two ways by which we can now proceed. The first one is that of pure consequentialism, in which we compare privacy and security solely based on their respective positive or negative consequences. The second strategy is that of comparing the right to privacy with the right to security, to find out whether they are the same kind of rights or not. I think the consequentialist approach is not suitable for the task of comparing privacy and security, so I will start by discussing that one.

The consequentialist approach only looks at the consequences of policy to determine whether it is acceptable or not. When comparing a right to privacy and a right to security, a consequentialist would only evaluate the outcome of the policy for the individuals involved. It usually does so in a strictly utilitarian way, with human welfare as the preferred way of measuring outcomes. Naturally, what the consequences are and how they are appreciated depends on a lot of factors: the status quo, the proposed policy, the preferences of the

individuals involved, and a lot of other elements. But let us try to look at privacy and security as objectively as possible. In the first chapter I have already given the positive consequences of privacy and security. Let us now compare them in a consequentialist way.

The point that immediately comes to mind is that a majority of people would probably value security more than privacy. This follows from the impressions that we get from the usual real life discussions on privacy and security: that it's not so bad that you are constantly being filmed by a surveillance camera if that means that your potential murderer is deterred by it and you will not be murdered. As noted before, though, this is a flawed comparison. We can safely assume that being murdered is the most extreme violation of your right to security imaginable; being filmed by one security camera is hardly the most extensive violation of your privacy. If you wish to objectively compare privacy and security you would have to compare being killed to something else, like being stripped bare and being displayed on a large public square so everyone could see you, while a loudspeaker is announcing your darkest secrets.

When we assess the consequences as listed in chapter one, we can see that privacy and security have a lot in common: both increase liberty in one way or another. If I enjoy security, I am able to do what I want to do without being murdered, robbed or beaten by the government or someone else. When I enjoy privacy something similar happens: when I am not under scrutiny I have more freedom to think as I want to think and act as I want to act. Enjoying privacy allows me to develop my individual self as I see fit, and that is definitely freedom. The difference between privacy and security is that privacy is primarily beneficial for psychological freedom, while security is primarily beneficial for physical freedom. They are both necessary conditions without which living a happy life is not possible. We are not able to determine whether security has more value than privacy or vice versa, because they are in many ways closely related to each other. Whether an individual prefers one over the other depends on his personality, his experiences and his preferences. The consequentialist approach for comparing privacy and security thus fails to give a satisfactory answer to our question.

So we have to look for our answer in a more deontological way. When distinguishing between different kinds of liberties, the difference between negative and positive liberty as defended by Isaiah Berlin is the most promising one. Berlin defines negative liberty as not being prevented by others from doing what you could otherwise do, and positive liberty as actually being able to do what you want to do. (Berlin, 1969, p. 122 & 131-132) In that sense,

both privacy and security are forms of negative liberty. They do not provide you with the opportunity to do something you otherwise couldn't have done, but merely ensure that others don't interfere with the things you could already do. In this sense, privacy and security are also more or less the same.

It is at this point that a very important distinction comes along. This idea, most notably defended by Quinn, deals with two different kinds of agency: action and inaction. (Quinn, 1989, p. 291) Quinn uses the terms active and passive for these types of agency, but in order to avoid confusion with Berlin's distinction of liberty I will use the terms active and passive. Active agency is doing something, passive agency is not doing something. The distinction between active and passive agency would be "the distinction between harm occurring because of what the agent does (because of the existence of one of his actions), and harm occurring because of what the agent did not do but might have done (because of the noninstantiation of some kind of action that he might have performed). (Quinn, 1989, p. 294) This argument is obviously deontological, because a consequentialist would not care between actions and inactions, but would only assess the consequences of the decision to act or not to act.

Quinn uses a strong *prima facie* argument in which he argues that passive agency feels different than active agency. I tend to agree with this. Killing a person by drowning him, or doing nothing while a person drowns, is both morally wrong. It violates the particular individual's right to life. However, the difference is significant. When I drown a person myself, I am actively causing him to die. Without my action, he would not have died. When I do not act while a person drowns, he dies without any involvement from me. If for some reason I would not have been there, he still would have drowned, because his drowning was caused by other factors than myself. This is not the case when I am actively involved in drowning him. Of course, it is still morally wrong to do nothing, and if we have to make the decision we should obviously come to the rescue of the drowning person. (Quinn, 1989, p. 302-305)

In general, especially democratic governments are susceptible to this kind of reasoning because of their responsibility to their citizens. In democracies, the government has legitimacy because individuals have given it to them through elections. And although I do not wish to get into consent theory, it should be noted that the power that a government wields is derived from the consent of the majority of its citizens. The government is to be held accountable for its actions and inactions by the electorate because the decisions that the government makes affect reality.

If we were to return to the natural state (whether it is Hobbesian or Lockean does not matter here), there is a certain situation that apparently needs to be changed (otherwise, there would be no need for a government). Because the government deliberately chooses every policy it enacts, it is responsible for the consequences of these policies for the lives of human beings.

However, the government is not to the same extent responsible for everything that happens that they could have prevented. It is not the United States government that is fully responsible for what happened on September 11, but the terrorists who planned and executed the attack. And although we may hold the government responsible for not preventing something that was caused by third parties, they are less responsible than they would have been had it been the result of a deliberate policy that they enacted. To take the September 11 example even further, it is quite easy to understand that American citizens would have been much angrier with their government if George Bush had ordered government employees to crash four planes in New York, Washington and Pittsburgh. The obvious reason for this is that generally we acknowledge that there is a fundamental difference between an act and an omission, especially when the consequences of that omission could not be foreseen.

Thus, what does it mean when we are facing a moral dilemma where we have to choose between violating one of two rights, one of them requiring active agency and the other one requiring passive agency? It definitely does not imply that the option that requires negative agency always overrules the other. It does mean that the right requiring active agency is more easily defeated than the right requiring passive agency: “The basic thing is not that killing is intrinsically worse than letting die, or more generally that harming is worse than failing to save from harm, but that these different choices run up against different kinds of right – one of which is stronger than the other in the sense that it is less easily defeated.” (Quinn, 1989, p. 289) Quinn is suggesting that *ceteris paribus*, when one can choose to violate right A by doing nothing or to violate right B by acting, we should always choose to do nothing.

And this is where we can start to see a huge difference between a right to privacy and a right to security. Of course, we can see both of these rights in a passive and active way. A negative right to privacy would indicate that nobody is eavesdropping on my private conversation (requiring an inaction), while a positive right to privacy would mean that someone (probably the government) would act to prevent someone else from eavesdropping

on my private conversation (requiring an action). The same goes for security: a negative right to security would mean that nobody is killing me (requiring an inaction), and a positive right to privacy would require that someone constrains another actor from killing me (requiring an action).

As we have established before, our discussion is about the government considering a policy that violates privacy in order to provide security to its citizens. This means that, although both privacy and security are negative liberties, we are now specifically discussing the dilemma between fulfilling a right to privacy through inaction, or fulfilling a right to security through action. If the government decides to do nothing, it is fulfilling a passive right to privacy (by not restricting it), but simultaneously neglecting an active right to security (by not preventing harm) through inaction. If the government decides to take the proposed measure, it is indeed fulfilling an active right to security (by preventing harm), but violating a passive right to privacy (by restricting it) through action.

The exact wording I use here is important. In both scenarios, one right is fulfilled. However, in the case of government inaction, the other right is 'neglected', while in the case of government action, the other right is 'violated'.

All in all, this leads us to two important conclusions for our comparison between privacy and security. Firstly, when the government wants to restrict privacy in order to protect security, the burden of proof that the privacy violation is justifiable lies with the government. This seems rather obvious to me, but in the public discourse the burden of proof is all too often placed with the people who refuse to have their right to privacy violated.

Secondly, it must be noted that when the government has to decide if they want to take a certain privacy-violating measure, it should *ceteris paribus* prioritize protecting privacy above protecting security. This is because the government is fully responsible for every privacy violation that is a result of the policy, but only partially responsible for every security violation that is a result of not implementing the measures.

Other things being equal, not violating the rights of citizens is more urgent than preventing the violation of their rights by other citizens. Logically, this does not indicate that privacy is always more important than security (remember that privacy is also not a trump card and we should take efficiency into account). In our hypothetical example of the decision to put security cameras in the street mentioned on pages 30 and 31, where we have quantified everything and have certainty of the outcomes, privacy is more important than security. So to come back to that example, if we want to reach an optimal equilibrium between privacy and

security, we will have to choose option C: government inaction.

5) How to make the privacy-security calculus

Of course, the example of policy options A, B and C was unrealistic. It is impossible to quantify rights like privacy and security in this way. But since we cannot do this in real life policy dilemmas, we do need to look at some form of calculus. This raises the following question: which factors should have weight in the decision?

First of all, and most significantly, quantities matter. If we take one of the many ethical dilemmas (for example, where we have to torture individual A so he can tell us the location of a ticking time bomb hidden somewhere in a large city), we can see that they do. The higher you raise the stakes, the more justifiable it becomes to violate an individual right. And although Henry Shue warns us of these hypothetical dilemmas because they are often too good to be true, we should definitely take into account how many individuals are affected by the decision that we make. (Shue, 2005, p. 231) Moreover, the sort of violation is also relevant. Judith Thomson illustrates this very effectively: "We have an intuitive notion of the strictness or, as I will say, the stringency of a claim." (Thomson, 1990, p. 153) She gives a fine example of two scenarios: one in which I have to kill A to save four people, and one in which I have to kick A in the shin to save four people. In both cases, if I choose to save the four people, A's right to security is definitely violated, but it is definitely violated *more* when I kill him than when I would kick him in the shin. So we could say that there should be a greater benefit (i.e. more people being saved) for me to be justified to kill someone than there would be for me to be justified to kick someone in the shin. Thomson: "In short, the size of the required increment of good seems to vary with the stringency of the claim: the more stringent the claim, the greater the required increment of good." (Thomson, 1990, p. 153)

Where precisely lies the breaking point where we can decide that the violation is justified or not? Thomson asks herself the same question, and answers it in the following way: "The answer is that there is no answer. There is no one size such that for any claim you choose, the claim is permissibly infringeable if and only if infringing it would generate an increment of good of that size." (Thomson, 1990, p. 153) So we can not point at some exact amount of lives that should be saved, for example, by a certain privacy-violating measure which has been taken. In practice, there are so many other factors weighing in when we have to make such a highly complex moral choice between violating privacy and allowing a violation of security to occur. Nevertheless, the understanding of how rights work that I have

given here definitely helps us understand how we should act when faced with such a complicated choice.

V. PRIVACY AND SECURITY FOR WHOM?

In the previous chapter I have provided a number tools that can be useful when comparing privacy and security. Clearly, these tools only apply to the rights of those that are involved. When a government has to decide about a policy that might violate privacy, we have to answer questions that will definitely affect the outcome of the decision process. The most vital one is: "who are involved in the policy?" The question is essential because policy that influences privacy and security affects the lives of a lot of individuals. Or, as Lucia Zedner puts it: "Given that sectional interests lurk below the surface of any claim to balance competing goods, we need in every case to ask not only what but *whose* interests we are weighing." (Zedner, 2005, p. 314) An analysis of the different groups and individuals that are involved goes much further than just counting how much individuals will benefit and how much will be disadvantaged. Besides, it cannot be settled by a vague reference to 'the common good'.

In this chapter I will explore the claim that privacy and security are common goods, and after that I will look at which relevant actors are involved when privacy and security change.

1) Do privacy and security belong to the common good?

Academic discussions about privacy and security are filled with talk about the common good of security and the individual good of privacy. In his book on privacy, Amitai Etzioni writes: "A good society seeks a carefully crafted balance between individual rights and […] the common good." (Etzioni, 1999, p. 5) This argumentation suggests that there is a fundamental difference in how we should look at privacy, which seems to be for the individual, and security, which seems to be for society as a whole. In this first part of chapter five, I will argue that this view on privacy and security is misleading and confusing, and that both concepts should be treated on an individual basis instead of a societal one.

How should we define the common good? Although there are a lot of definitions available for what the common good is, and the subject is not without controversy among authors, I will use one that is adequate for my purposes. The common good, I would argue, is the good and well-being of a society as a whole. This means that we can think of certain actions or decision as beneficial or detrimental for society as a whole, thereby increasing or decreasing the common good. For example, we might argue that freedom of speech benefits the common good since it will allow our society to be an open one, with a lot of room for

democratic debate.

The common good is often presented as being beneficial to everyone involved. Let us look at the example of freedom of speech: we might argue that everyone in our society benefits from living in an open society with ample room for democratic debate, and that people are content when they can voice their opinion, and unhappy when they are not. In the debate about privacy and security, the right to privacy is often displayed as an individual right, with security being labelled as part of the common good. Thus, installing security cameras will benefit the greater good because it will make our society safer and therefore the common good is increased. Refraining from installing security cameras will do just the opposite and accordingly will decrease the common good, the argument goes.

In my view, this argument is wrong for at least two reasons. First of all, if we would accept that security is beneficial to the common good, we also have to accept that privacy is beneficial to the common good. Privacy allows individuals to have a realm of their own where they can escape public scrutiny, which increases their happiness. So a legal right to privacy that is not violated by the government generally will also increase the public good.

Secondly, I believe that if we take measures that change the status quo, we should not be looking at them as a general increase of the public good. We should be looking at them as an increase of a certain good for certain individuals. So if I am a member of a community, and we can establish there is a common good, that good should also benefit me. If it doesn't, it either means that I am not a member of that community or that in the end the good is not common: we can only call something 'good' if it benefits me. If it doesn't benefit me, it isn't a good for me. It might be a good for my neighbour and for every other inhabitant of the city where I live, but if it doesn't positively affect my own situation it would be wrong to say that I just received a good.

Let us look at a specific example. We might say that having more police officers on our streets is beneficial for the common good, because everyone will be safer. I would argue that this is not true. We can have a higher *expectation* of safety, but in the previous chapter it was already argued that we do not have a right to a feeling of safety, but only to true security through physical integrity and property protection. If the additional police officers have no concrete effect at all on my situation it is impossible to claim that I have benefited. Sure, it might seem nice that there are more police officers, but if I still get robbed when the police officers aren't looking I have not benefited from any good. In the end, the situation might even have become worse for me (for example, because one of the extra police officers is a

rookie and accidentally shoots me while I am jogging). It would be illogical to call this a common good. Of course, this doesn't mean that it's a bad policy, it just shows that we should be extremely careful with the concept of a common good. It is very easy to assume that something that we call a common good is good for everyone in a society, while actually it only benefits a few. This is especially relevant for the debate on privacy and security.

In the end, the common good is nothing more than the aggregate of individual goods. Indeed, the common good can be said to benefit all of us, but the only actors that we are dealing with are individual ones. "Society" is a human construct that is nothing more than a group of individuals that have something in common (usually the country in which they live) and which is only made up of the individual members. In the same way, a common good is nothing more than the aggregate good of these individual members. When we are considering policies that affect privacy and security, we should always consider who are involved.

2) Who are involved with privacy and security?

It follows that privacy and security should be treated as goods that affect individuals, and not communities or societies. The next question then is: "which individuals?" If the government is proposing a law that increases security but decreases privacy, which individuals should we take into account while deliberating on the desirability of the particular law?

I will start by discussing which people are influenced by a change in security. Let us return to our example of a government proposal to install surveillance cameras in the hypothetical shopping street with a moderate amount of crime. And let us assume that it is proven that for this particular street, the surveillance cameras will lead to a certain reduction of crime, because they act as a deterrent for criminals who don't want to be caught on camera while beating up a tourist or stealing a purse.

We could argue that we have just increased security for everyone who lives in the street or passes there, and hence the common good of security has been increased. I disagree with this argument. When I am walking through this street at night, and I won't get robbed or molested whether there are surveillance cameras or not, my security has not increased since nothing has actually changed for me. The same thing is true when I am going to be robbed or molested anyway: when something doesn't affect me at all, how am I to be considered as a relevant actor in the deliberation process for the policy?

We can think of it more schematically in the following way. Let us assume that

everyone who passes through our street has an amount of security that we call S_1 before the surveillance cameras are installed. S_1 is not the amount of security you can expect, but the actual amount of security that you are going to have when walking down the street. This means that someone who will get murdered in the street will have a very low S_1, while someone who will walk down the street safely will have a very high S_1. It also means that we can't really know in advance how much S_1 anyone has. The situation changes, however, when the surveillance cameras are finally installed. Everyone who now passes the street has S_2 security. When S_1 and S_2 are the same for an individual, this means that his security has not increased and he has not benefited from any good, common or not. So I would argue that for us to talk about a good, it should affect our situation in a positive way.

Our *expectation* of security might increase because we understand there are a number of cameras installed and we expect them to deter criminals from robbing or killing us. We could say that this increase in expectation of security is a good, because anyone who knows about these cameras has an increased feeling of security. However, this is not very significant for our discussion about the desirability of surveillance cameras, since this effect will become less over time when people learn that these cameras are ineffective. And even if that would not be the case, we should still follow Etzioni's rule that the government should try to find alternatives that do not violate privacy, which I think is possible in the case of an expectation of security.

What are the consequences for our discussion about the actors involved in increases or decreases of security? It means that the argumentation above radically changes the general image that we have of these measures. If we only consider the people whose S_2 is higher than their S_1 in our calculus on whether the privacy-violating policy is acceptable or not, there are fewer people to consider as beneficiaries to this policy.

In the context of September 11, this also leads to fundamental changes. In the legislation that followed the terrorist attacks, many civil liberties were constrained in the name of the public good of security. This was presented as beneficial for every American citizen. What if this legislation had been passed before September 11, and would have prevented the attacks? Basically, it would have meant that although over 300 million Americans had been constrained in their liberties to provide a better S_2 for just over 3000 people. Now, I am not arguing that this legislation shouldn't have been there before September 11 to prevent the truly tragic loss of life. I do think, however, that this drastically changes the way we look at considerations that involve concern for the common good, or concern for the good of an enormous amount of people. It seems the reason that measures

claiming to promote the common good are so popular among a lot of people is because of the high level of uncertainty. You never know if you are the one who is going to be murdered under S_1 but will survive under S_2. I am convinced that his hope for a possible better situation is a major reason for a lot of individuals to willingly give up their privacy and other civil liberties in exchange for these security-enhancing measures.

But what about privacy? Does that work the same way as security? I would argue that it does, but there are two differences that must be discussed here. The first difference is that often a lot more individuals are involved than noted in the considerations about security above (which we can see from the example of 300 million individuals versus 3000 individuals). In the case of the surveillance cameras, the policy decreases the privacy of everyone who is being filmed in the street. This means that everyone's P_1 will drop to a lower P_2 when the surveillance cameras are installed. How much it drops depends on what is being done with the images that the cameras capture, but it is undeniable that everyone who gets filmed has his privacy reduced.

To conclude this chapter, it must be underlined that a lot of discussions about privacy and security are conducted in the wrong way by displaying privacy as something that only benefits one individual, while security benefits everyone. It was observed that security only benefits those whose situation is actually affected. Surveillance cameras that allegedly reduce crime in Amsterdam, for example, cannot be said to increase my security because I never go to Amsterdam. And cameras that are placed in an area where previously there was no crime at all also do not increase security because the status quo does not actually change. Thus, when discussing specific policy measures to increase security, we should always consider who are involved in a different way.

VI. CONCLUDING THOUGHTS

In my thesis, I have tried to answer the following question: *which conditions should be fulfilled for governments to be justified to restrict the privacy of individuals?* Unfortunately, the answer to this question is not a neat checklist with a number of conditions that have to be fulfilled, with the indication that when these are fulfilled, the government is justified to restrict the privacy of individuals in order to improve security. Real life cases are too complex for such a simple checklist, and decisions should always be made with regard of the context.

There are, of course, some rules that the government should follow when they restrict privacy. Authors like Westin and Etzioni have introduced such rules, by stating that there should actually be an improvement of security before privacy may be restricted, and that the measure should be as minimally intrusive as possible. Governments should follow these rules, but that still does not help them in dilemmas where they have to choose between defending security and defending privacy.

In this thesis I have tried to show that the way how governments look at restricting privacy can be improved. By viewing security and privacy as more than just goods that the government should provide for its citizens, but as rights that every individual has. I have argued that we have a right to privacy and a right to security, and that both of these rights can be defended from a consequentialist point of view and a deontological one. And when there is a dilemma between defending one right or the other, I think that actions that violate rights need a stronger defense than inactions that violate rights. Governments therefore have more responsibility for the consequences of their actions than for the consequences of their inactions. This means that they have more responsibility for the violations of the right to privacy than for the violations of the right to security that are committed by other agents.

Governments should also look closely at whose rights are actually involved in the decision. In a lot of cases privacy is displayed as an individual good while security is displayed as a common good, which would make it somehow more important than privacy. Contrasted to this, I have argued that the only actors involved are those who are being affected by the privacy-violating measure: only people whose right to privacy is violated and only people whose security is being increased. The common good, and individuals who are not affected by the government measure, do not play a role in the discussion about it.

The burden of proof that the privacy violation is justifiable in light of the alleged consequences lies with the government, not with any citizens who might object to their right to privacy being violated.

It must be admitted that making these decisions is hard, but that is because the stakes are high and there are fargoing consequences for a lot of people. In the end, I think that a majority of privacy-violating measures that are in effect in numerous countries at this moment, would not pass a thorough examination of whether they are justified or not. As a matter of fact, there are a lot of these measures that will be justified, and they are very important for everyone because they are preventing the violation of the right to security. I hope that the conclusions of my thesis can serve as a different way of how governments look at privacy-violating measures.

A lot of work needs to be done, though. Privacy and security are very important issues, and no government should take measures that violates rights lightly. For future research, I believe two things would improve the way we deal with privacy in Western countries even more. First of all, we need to determine what types of private information we should protect via a right to privacy. This is not an easy task, and I have given some pointers of how it can be done in chapter III. Secondly, existing government policies that violate the privacy of individuals should be evaluated. Their effectiveness should be tested, and we should determine whether the violation of the right to privacy that they cause is justified. If this is done, I believe we can really change Western democracies to countries where the right to security is protected and the right to privacy is respected. Or, to return to the metaphor of Bentham's Panopticon, we can realize societies where individuals are not treated as prisoners that need to be under continuous observation.

LITERATURE

Berlin, Isaiah. Four Essays on Liberty. London: Oxford University Press, 1969.

Bloustein, Edward. “Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser.” New York University Law Review (1964): 962-1007.

DeCew, Judith. In Pursuit of Privacy. Law, Ethics, and the Rise of Technology. Ithaca: Cornell University Press, 1997.

DeCew, Judith (2002). Privacy, in: Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/archives/fall2011/entries/privacy/. Visited on December 20th, 2011.

Etzioni, Amitai. The Limits of Privacy. New York: Basic Books, 1999.

Gavison, Ruth. “Privacy and the Limits of Law.” The Yale Law Journal (1980): 421-471.

Hart, Herbert. The Concept of Law. Oxford: Clarendon Press, 1961.

Hobbes, Thomas. Leviathan. New York: Dover, 1651.

Hohfeld, Wesley. Fundamental Legal Conceptions. New Haven: Yale University Press, 1923.

Mill, John. On Liberty. London: Penguin Books, 1859.

Parent, William. “Privacy, Morality, and the Law.” Philosophy & Public Affairs (1983): 269-288.

Quinn, Warren. “Actions, Intentions, And Consequences: The Doctrine of Doing and Allowing.” The Philosophical Review (1989): 287-312.

Scanlon, Thomas. “Thomson on Privacy.” Philosophy & Public Affairs (1975): 315-322.

Semple, Janet. Bentham's Prison: A Study of the Panopticon Penitentiary. Oxford: Clarendon Press, 1993.

Shue, Henry. "Torture in Dreamland: Disposing of the Ticking Bomb." Case Western Reserve Journal of International Law (2005): 231-239.

Solove, Daniel. "Data Mining and the Security-Liberty Debate." The University of Chicago Law Review (2008): 343-362.

Spinello, Richard. "The End of Privacy." The New Republican (1997) vol. 176 (1): 9-13.

Sumner, Leonard. The Moral Foundation of Rights. Oxford: Clarendon Press, 1987.

Thomson, Judith. "The Right to Privacy." Philosophy & Public Affairs (1975): 295-314.

Thomson, Judith. The Realm of Rights. Cambridge: Harvard University Press, 1990.

Waldron, Jeremy. "Security and Liberty: The Image of Balance." The Journal of Political Philosophy (2003): 191-210.

Walzer, Michael. "Political Action: The Problem of Dirty Hands." Philosophy & Public Affairs (1973): 160-180.

Warren, Samuel & Louis Brandeis. "The Right to Privacy." Harvard Law Review (1890): 193-206.

Wenar, Leif (2005). Rights, in Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/archives/fall2011/entries/rights. Visited on May 14th, 2012.

Westin, Alan. Privacy and Freedom. London: The Bodley Head, 1967.

Westin, Alan. "Social and Political Dimensions of Privacy." Journal of Social Issues (2003): 431-454.

Zedner, Lucia. “Securing Liberty in the Face of Terror: Reflections from Criminal Justice.” Journal of Law & Society (2005): 507-533.