Just Surveillance?

Kevin Neil James Macnish

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds

School of Philosophy, Religion and the History of Science

August, 2013

The candidate confirms that the work submitted is his/her own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

I would like to thank my three supervisors, Rob Lawlor, Chris Megone and Robin Le Poidevin for their help in writing this thesis. Rob's tireless efforts to support and challenge me over the last few years have been particularly appreciated. I would also like to thank Barbara, Christopher and Helena for their unwavering support and uncomplaining willingness to see me disappear into my study on too many evenings and Saturday mornings.

Abstract

There is little written specifically on the ethics of surveillance. David Lyon has proposed three categories of concern (Lyon 2001), John Kleinig five (Kleinig 2009) and Gary Marx twenty-nine (Marx 1998). However, these categories are rarely defined or defended philosophically and lack any underlying ethical theory. Further, while Lyon, Kleinig, Marx and others have elements in common, each raise issues that the others neglect.

I argue that the just war tradition can form a framework by which the ethics of surveillance practices may be judged. This separates out questions of who is conducting surveillance, why they are doing it, whether surveillance is proportionate, whether it is necessary, and what its chances of success are. Questions are also raised regarding the ability to discriminate and the proportionality of the means of surveillance. Thus this framework raises *all* the questions which should be asked of an ethical approach to surveillance and neglects none.

We can also employ the just war tradition to inform the content of the debate. For example, how discrimination is dealt with in war could be instructive as to how it should be employed in surveillance. This tradition thus provides a rich, relevant and long-lived discourse on which to found an ethics of surveillance.

Table of Chapters

Table of Contents

List of Tables

Part I - Surveillance and War

1. Introduction

There has been a marked increase in the use of surveillance in democratic countries such as the UK and USA in recent years. This is due in part to the development of technology that enables surveillance to be undertaken more easily, cheaply and widely than before, and in part to the threat to society perceived in the wake of the 9/11 and 7/7 terrorist attacks. However, there have been few attempts to develop a systematic ethic of surveillance. This thesis sets out to do that, drawing on the just war tradition as a model. Using this model I will provide a framework by which applications of surveillance may be assessed and, in such cases as is necessary, limited or refined.

The papers that do tackle the need to establish an ethic of surveillance tend to suffer from a lack of theoretical structure or overall coherence. For example Gary Marx, in his *Ethics for the New Surveillance* lists 29 principles for consideration (Marx 1998). Aside from the fact that this makes for an unwieldy checklist, Marx acknowledges that the paper contains a mix of first principles and empirical consequences, and that it lacks any formal normative argument offering justification for those principles. Marx responds that such an argument would be a Rosetta stone to philosophers working in this area. While Marx's principles are unquestionably helpful, I believe that they are captured in the principles laid out by the just war tradition, which also provides the normative structure that Marx's approach lacks. Moreover, by appealing to the just war tradition, we are able to ground the ethics of surveillance in a rich philosophical tradition. Many of the relevant principles have received centuries of attention insofar as they apply to war. If they can be successfully transferred to the arena of surveillance then we stand to benefit enormously from the insights of this philosophical tradition.

My aim in the thesis is threefold. First, to convince the reader that the just war tradition provides an adequate framework for the evaluation of surveillance from an ethical perspective, capturing all of the concerns raised by others in the field and missing none out. The framework that I propose will provide necessary and sufficient conditions for acts of surveillance to be ethical. Second, I will demonstrate that the tradition provides a rich discourse from which one can draw in order to inform the debate surrounding ethical surveillance. There are many considerations such as discrimination and proportionality

which are explored in the just war tradition both historically and in the contemporary context. By appealing to the writings in this tradition I inform the debate without needing to reinvent the wheel in the context of surveillance. For example, the principle of proportionality as it pertains to surveillance, I argue, can benefit from a consideration of how the principle of proportionality pertains to warfare. Third, I shall argue in each case for a conclusion as to how surveillance can and should be employed through reference to these principles.

The three aims are not mutually dependent. It is possible to accept my conclusions regarding a proposed *framework* for consideration, for example, while still holding that the just war tradition has little to say on the *content* of the ethical principles as they pertain to surveillance instead of war. Alternatively the tradition may be felt to have much to say on the content of these principles in surveillance but nonetheless overlook certain areas such that it fails to provide a complete ethical framework which captures all the salient ethical concerns and leaves none out.

My aim is not that the application of the just war tradition to surveillance will be the final word on the matter. The just war tradition does not claim to say everything that can be said about justification in war. For example, some questions are not philosophical but rather empirical, and hence better treated by psychology or sociology. The tradition offers a framework for ethical discussion rather than the data which populate that discussion. It does not, for instance, tell us that landmines blow children's legs off, but rather that something which harms children in warfare is wrong. Similarly if anthrax were somehow discriminating in whom it affected it might still be argued that it is a morally unacceptable means of conducting war. The just war tradition will not always say outright why this is the case, but it will provide a framework with which to discuss it.

The same is true in developing a framework for the analysis of the ethics of surveillance. What I propose as a framework will not inform the reader which harms are occasioned by particular forms of surveillance. What it will do is enable an analysis of the ethics of using those forms given the harms which have been established by empirical research. Similarly if acts of surveillance are suspected to be ethically dubious it will provide a structure which can be employed to analyse whether and why those acts really are unethical.

The just war tradition is itself not without controversy. Each of the principles raised in the tradition has been contested. Whether these principles really do pertain to the ethics of war is not my concern here, but rather whether these elements pertain to the ethics of surveillance. However, it is because of these controversies that the issues raised in the just war tradition have been discussed throughout its history. The tradition therefore contributes a significant body of moral discourse to the debate from which one can draw. As Nietzsche saw, while philosophers might believe that their success lies in the buildings they construct, posterity might demonstrate that the real value lies in the bricks they used. We can as often as not build as much from the ruins as from the successes of their work (Nietzsche & Hollingdale 2005 p. 33).

1.1 Objections

Some might object to making comparisons between war and surveillance. In war people die or are physically injured, not to mention raped, starved, displaced, etc. In the case of surveillance the associated harms, while they may be real enough, are not as severe. This is not the only disanalogy, but it is a key consideration. To that end it is important to stress at the outset that I am *not* attempting to draw a parallel between war and surveillance. I accept that there are obvious disanalogies: to be subject to surveillance is unquestionably different from being subject to warfare.

By contrast, what I am saying is that there is an analogy between the *ethics* of war and the *ethics* of surveillance. The analogy is not perfect. One cannot just take the principles as applied to warfare and, like a cookie-cutter, apply them to surveillance. However, it is possible to reshape those principles so that they provide an effective framework for analysis of acts of surveillance. Through considering the principles pertinent to the ethics of war it will be possible to develop a robust methodology for assessing the ethics of surveillance.

A second possible disanalogy concerns consent. While two states may declare war on each other it is unlikely that they have both freely chosen that course of action. More typically one state is likely to feel constrained to act because of the (perceived) actions of the other. Surveillance, on the other hand, may result from a free choice. If a person consents to surveillance, or even requests it (imagine here contestants in the televised game show Big Brother), then is there harm in that surveillance? Questions of consent, including consent

to be harmed, and the possibilities of exploitation and coercion are considerably larger than the scope of this thesis. As a result I will focus here on non-consenting surveillance. Here I take non-consenting surveillance always to be *pro tanto* harmful, based on a list of what I take to be plausible harms which are discussed in chapter 3. The questions raised in the rest of this thesis will seek to ascertain whether and when these *pro tanto* harms can be outweighed.

There are hence at least two possible disanalogies between surveillance and war regarding harm and consent. As noted above, though, this thesis does not seek to draw an analogy between war and surveillance but between the ethics of war and the ethics of surveillance. These disanalogies do not therefore defeat the aim of the thesis.

A further objection may be levelled that I am ignoring consequentialist considerations in seeking justification for surveillance. This is true. While the just war tradition considers consequences as an aspect of proportionality, it is not a consequentialist theory. Such approaches have been suggested, or at least hinted at, by George Mavrodes and R.B. Brandt (Mavrodes 1975; Brandt 1972). These are atypical of the overall tradition, though, and it is the typical position put forward by that tradition which holds the greatest promise for the ethics of surveillance. As such I focus on the traditional position rather than spend time considering consequentialist alternatives.

A second reason for rejecting a consequentialist approach is its failure to respect individuals, particularly as seen in the problem of distribution. The failure to respect individuals is, as Rawls has argued, a problem common to all purely consequentialist accounts (Rawls 1999). In terms of surveillance, such an account threatens both the autonomy and the dignity of the individual though eroding the individual's privacy. Imagine that universal surveillance is justified in terms of security: a net social benefit of security outweighs any individual's interests in privacy, and so privacy is eliminated in a manner similar to that explored in Orwell's *1984* (Orwell 2004). In such a situation the individual ceases to be free to do, or even to think, what they want. This is true even within what a liberal society might term "reasonable limits". Hence, to continue the analogy with *1984*, if the individual wishes to keep a diary even this may not be kept secret from the state. This is a clear infringement on the individual's autonomy. There are further harms to

dignity if the vigilance of the state intrudes into all areas of the individual's domestic life, to observe that person naked, having sex or using the toilet.

The harm to an individual's privacy is not automatically wrong. It may be that the individual has in some manner deserved these harms. However, the problem with a pure consequentialist account is that it is blind to which individuals are harmed and which are not. If invading the privacy of an innocent few increases the net benefit to society (i.e. through serving as a deterrent to others who might threaten the state) then to the consequentialist that invasion is justified. Yet this is a conclusion which I find reprehensible. Justice surely involves treating all people equally and fairly, and this approach does neither.

This is not meant to be the final word on the debate regarding consequentialist versus deontological ethics. Indeed, it is hardly even an opening of the discussion, which goes beyond the scope of this thesis. It is rather intended to briefly explain my position, and my reason for taking it. I do hold that it is important to consider consequences as part of an overall justification. This, as I have mentioned, is encapsulated in the proportionality condition of the just war tradition.

1.2 Structure

Surveillance can cover a broad variety of approaches from the long-range telephoto camera and CCTV to phone-tapping and hacking e-mail accounts. It may be used to capture a criminal in the act of committing a crime, or to deter that criminal from acting in such a way in the first place. It may also be used for commercial purposes, tracking the purchase history of a customer, or health concerns in monitoring an infirm patient in a care home. Throughout this thesis I shall consider each of these insofar as the subject of the surveillance has not consented to that surveillance.

In questioning any act one must ask the standard questions of who, what, why, where and when (Toner 2010). The just war tradition asks these questions in a particular manner which, I argue, is highly pertinent to the discussion surrounding surveillance. I develop this argument in Chapter 2.

Having established that it is at least *prima facie* plausible that the just war tradition be employed as a tool for understanding the ethics of surveillance (chapter 2), and that there is *pro tanto* harm associated with surveillance (Chapter 3), I develop each of the nine principles of the just war tradition in its own chapter. I turn first to the question of *jus ad bellum*, the justification of going to war, or in this case *jus ad speculandum*, the justification of employing surveillance. The principles considered here are: justified cause (chapter 4), correct intention (chapter 5), authority (chapter 6), necessity (chapter 7), formal declaration (chapter 8), chance of success (chapter 9) and proportionality (chapter 10). I then consider the issue of *jus in speculando*, the justification of the methods employed in surveillance. Here there are two major principles (proportionality of means and discrimination) and two minor principles (means *mala in se* – inherently evil – and treatment of prisoners). Whether or not the minor principles should be included in the just war tradition is a matter of dispute. All commentators agree that the major principles are correctly applied in considerations of *jus in bello* but only some believe that the minor principles should also be considered. In this thesis I address only the major principles of proportionality of means (chapter 11) and discrimination (chapter 12). The minor principles may provide short-cuts but do not add fundamentally new insights to the framework and so are not necessary to the overall thesis.

The core position for which I shall argue is that the majority of the principles discussed are necessary for surveillance to be justified. The principles which are not necessary are authority and formal declaration. The reasons for this are too complex to be dealt with in an introduction, but shall be explored further in chapters 6 and 8. Otherwise I hold that there must be a justified cause, supported by a correct intention, that the surveillance must be necessary and have a chance of success, and that it be proportionate. In terms of *jus in speculando*, methods of surveillance should again be proportionate in the harm that they occasion and they should seek to discriminate as much as possible between legitimate and illegitimate targets. Again, each of these will be considered in greater depth in their respective chapters.

Individually the principles do not amount to sufficient justification for surveillance. Taken together they do provide sufficient justification. That is, if an act of surveillance can be shown to meet the requirements of the seven principles of *jus ad speculandum* and the two

major principles of *jus in speculando* then that act will be justified. Indeed, this is a central feature of my argument: that taken together the nine principles of just surveillance provide the necessary *and* sufficient conditions to justify an act of surveillance.

2. Just Surveillance?

I noted in the introduction that there are papers which attempt to establish an ethics of surveillance. However, I claimed, these tend to suffer from a lack of theoretical structure or coherence. In this chapter I shall also argue that they lack comprehensiveness in that some authors include principles which others ignore. I start by considering the contribution made by these authors. From there I develop the argument introduced in the introduction that by drawing an analogy with the ethics of war a framework can be developed for analysing the ethics of surveillance. This framework will be considerably more comprehensive than anything yet suggested because it includes all the relevant considerations and misses none of them out. Furthermore, through drawing on centuries of discussion regarding the ethics of war, it provides a significant body of philosophical discussion surrounding each of the principles involved. This provides a running start to a relatively new discussion regarding the ethics of surveillance.

2.1 Literature Review

David Lyon suggests a possible grounding for surveillance ethics in the notion of personhood, drawn largely from the work of Emmanuel Levinas and Zygmunt Bauman (Lyon 2001). His use of personhood rather than privacy stems from sociological concerns regarding the manner in which the term privacy is or has been used. In this regard Lyon's work is similar to that of Graham Sewell and James Barker, who concern themselves primarily with privacy in the workplace (Sewell & Barker 2001). They employ Foucauldian terms of power/knowledge and "rules of right", an establishment of rights that are granted in different contexts. In both of these cases the authors seek to establish what is wrong with surveillance before going on to suggest a basic ethical framework against which surveillance may be assessed.

Anita Allen takes a different approach to the question without suggesting the need for a framework as such (Allen 2008). Establishing first that surveillance is not inherently unethical she looks at a series of scenarios, starting with the smallest scale (self-interest and parental monitoring) and ending at the largest (state security). Throughout she draws on real world scenarios to make her point and appeals to an intuitive response. While this grounds the argument in reality, it risks the reader withholding judgement due to paucity of

information in the particular cases, or simply disagreeing. She also raises or alludes to a number of questions which she fails to develop, such as the ethical significance of who is carrying out the surveillance, why they are performing this action, and whether the surveillance is necessary. Furthermore, Allen highlights the distinction between the justification of the decision to employ surveillance and the justification of the method of surveillance used, but she does not develop this in the paper. While Allen mentions this distinction only in passing, I will argue that this distinction is important. Allen also fails to address several further concerns, such as proportionality and surveillance of the innocent.

In this last area Allen is not alone. Few of the commentators considered above take into account the ethical issue that arises when the innocent are made the objects of surveillance. Rather, and operating with the benefit of hindsight in legal cases, for Allen it seems as if guilt is assumed. However, surveillance is often undertaken with the aim of *establishing* guilt. In these cases the decision to employ surveillance must be based on suspicion rather than firm evidence, and so we need to ascertain the warrant for that suspicion and the distinction between legitimate and illegitimate targets in these cases.

There is also the question of different kinds of surveillance, which is often overlooked. There is clearly a difference between standing on tip-toe outside someone's bedroom window and operating a multi-billion dollar signals intelligence organization such as the National Security Agency. Furthermore, these different kinds of surveillance will yield different levels of information, from a single blurry photograph, inadmissible in court due to its lack of clarity, to full video and audio capture of a person's life over a period of time.

A further concern arises from the questions of what information is gathered, and to what extent is that information relevant to the justifying cause? In the case of surveillance, extraneous information will be gathered alongside that which is relevant to the case at hand. To what extent should this be a concern, and what lengths should be undertaken to minimize the collection of such extraneous information? Indeed, should such lengths be taken, given that information might only be seen to be extraneous after the surveillance operation is complete, if then? Additionally, how should any information collected through surveillance be used, stored and protected?

These questions regarding justification, proportionality and a perceived need for discrimination will turn out to be well answered by an application of the just war tradition. Before turning to this, though, it is worth pausing to summarise the principles of ethical assessment offered by existing approaches in the academic literature. In particular, I wish to consider those proposed by Lyon, Sewell and Barker, John Kleinig, Gary Marx and the principles set out in the UK's Regulation of Investigatory Powers Act (RIPA 2000).

Lyon lists three principles: participation, personhood and purpose (Lyon 2001). By participation I take him to mean those involved in the decision-making process: is it democratic and accountable. (This touches on questions of the authority of the surveillant to carry out the surveillance.) Personhood looks at how the surveillance affects the individual or group surveilled, a subject which Lyon has pioneered through recognition of the social sorting effect of surveillance. I see this as the harm visited by surveillance on those it affects, and the need for any such harm to be held in proportion to the justifying cause. Finally, Lyon's consideration of purpose analyses the justifying cause for the surveillance: why is surveillance being undertaken in the first place.

Sewell and Barker similarly recognise authority and justifying cause as issues in surveillance, but do not look at proportionality as a separate principle (Sewell & Barker 2001). Rather they focus on necessity: is the act of surveillance really necessary or could a less intrusive measure be employed? This does touch on proportionality and harm, but contains significant differences. An act may be proportionate but not necessary, or it may be deemed necessary to achieve a desired end but not be proportionate to that end.

The Regulation of Investigatory Powers Act (RIPA) recognizes this distinction in that it employs the notions of proportionality (shared with Lyon) and of necessity (shared with Sewell and Barker) as separate issues (RIPA 2000, 29(2)). The Codes of Conduct derived from RIPA also introduce a third consideration of discrimination: that surveillance should focus on the intended target as much as possible and seek to limit the monitoring of unintended targets (Home Office 2010, 3.8-3.11). Furthermore, as state legislation seeking to regulate the actions of public bodies, I take it that some notion of authority is assumed, albeit not explicitly stated.

John Kleinig has produced what to me is the most comprehensive purely normative list to date (Kleinig 2009). He lists cause, necessity and proportionality, separating the latter into the areas of proportionality of ends and proportionality of means. He also discusses the need for there to be a reasonable chance of success and a prohibition on means *mala in se*. That is, means which are evil in themselves and should thus never be used. In conventional warfare such means have been seen to include certain chemical and biological weapons, and increasingly anti-personnel landmines. In this Kleinig comes extremely close to my own position which I shall develop below of explicitly using the just war tradition to inform his position. Given that he is writing with practitioners in mind, and particularly the police, Kleinig takes authority as a given.[1] However, his position fails to take into account discrimination which, as seen above, is included in the ethical principles of others as well as being one of the best established principles in the just war tradition.

Finally, Gary Marx has offered a list of 29 principles combining normative and empirical considerations (Marx 1998). In brief, I believe that he employs the following concerns: authority, intention, cause, necessity, declaration of intent, reasonable chance of success, and proportionality of both ends and means. These can be seen from the following, in which I quote Marx's principles rearranged under the criteria of just war principles to demonstrate the correlation:

> *Authority*
>
> 10. Public decision-making: Was the decision to use a tactic arrived at through some public discussion and decision-making process?
>
> 12. Right of inspection: Are people aware of the findings and how they were created?
>
> 13. Right to challenge and express a grievance: Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?
>
> 14. Redress and sanctions: If the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behaviour?
>
> 16. Equality-inequality regarding availability and application:
>
> > (a) Is the means widely available or restricted to only the most wealthy, powerful, or technologically sophisticated?

[1] I am grateful to John Kleinig for personal correspondence which clarified this aspect of his argument.

(b) Within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist?

(c) If there are means of resisting the provision of personal information are these means equally available, or restricted to the most privileged?

Intention

15. Adequate data stewardship and protection: Can the security of the data be adequately protected?

27. Information used for original vs. other unrelated purposes: Is the personal information used for the reasons offered for its collection and for which consent may have been given, and do the data stay with the original collector, or do they migrate elsewhere?

28. Failure to share secondary gains from the information: Is the personal data collected used for profit without permission from, or benefit to, the person who provided it?

Just Cause

7. Consent: Do individuals consent to the data collection?

8. Golden rule: Would those responsible for the surveillance (both the decision to apply it and its actual application) agree?

20. Beneficiary: Does application of the tactic serve broad community goals, the goals of the object of surveillance, or the personal goals of the data collector?

25. Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate?

26. The goodness of fit between the means and the goal: Is there a clear link between the information collected and the goal sought?

Last Resort/Necessity

22. Alternative means: Are other, less costly means available?

23. Consequences of inaction: Where the means are very costly, what are the consequences of taking no surveillance action?

Formal Declaration

6. Awareness: Are individuals aware that personal information is being collected, who seeks it, and why?

Chance of Success

5. Invalidity: Does the technique produce invalid results?

26. The goodness of fit between the means and the goal: Is there a clear link between the information collected and the goal sought?

Proportionality (of decision to use surveillance)

1. Harm: Does the technique cause unwarranted physical or psychological harm?

2. Boundary: Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?

3. Trust: Does the technique violate assumptions that are made about how personal information will be treated, such as no secret recordings?

9. Minimization: Does a principle of minimization apply?

19. Negative effects on surveillants and third parties: Are there negative effects on those beyond the subject and, if so, can they be adequately mediated?

29. Unfair disadvantage: Is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?

Proportionality (of method of surveillance employed)

21. Proportionality: Is there an appropriate balance between the importance of the goal and the cost of the means?

24. Protections: Are adequate steps taken to minimize costs and risk? (Marx 1998)

There are four questions which Marx raises which do not fit into the framework of the just war tradition. These are as follows:

4. Personal relationships: Is the tactic applied in a personal or impersonal setting?

11. Human review: Is there human review of machine-generated results?

17. The symbolic meaning of a method: What does the use of a method communicate more generally?

18. The creation of unwanted precedents: Is it likely to create precedents that will lead to its application in undesirable ways? (Marx 1998)

While these are interesting questions, their normative thrust is not always clear. Human review of machine-generated results (Question 11), for example, will be discussed in chapter 9 (Chance of Success), where I argue that a fully automated (i.e. non-human) review may be beneficial in some cases but not others. Similarly the consideration of personal or impersonal settings (Question 4) may have different preferences depending on the context. Physicians may be expected to deal with personal information as relating to a known individual. Bureaucrats, on the other hand should normally deal with the same information impersonally, so as to avoid bias or conflicts of interest. Question 17 does not, as I read it, involve an ethical position. However, it could be reworded to read, "does the method communicate [something unethical]?" In this case it could then be seen as falling under authority (if the unethical object communicated relates to the surveillant) or

proportionality (if the unethical object communicated harms the surveilled subject) or possibly means *mala in se* (if the unethical object communicated is so objectionable that it should never be communicated under any circumstances). Question 18 could be treated similarly (i.e. falling under authority, proportionality or means *mala in se*). However, the likelihood of creating precedents does not in itself make something ethically objectionable. Certainly if it *does* set a precedent and future developments are unethical then those developments would be wrong (by definition). However it seems feasible that an ethical act which one is duty-bound to perform may create such precedents. If so then it is the unethical future acts which are wrong and not the initial act itself.

Hence Marx includes questions relating to authority, intention, cause, necessity, declaration of intent, reasonable chance of success, and proportionality of both ends and means. Significantly, though, Marx fails to deal with the issue of discrimination, which I hold to be a key concern.

In summary, each of the above authors holds a part of the jigsaw, but none is able to complete the picture. A cursory glance at the list of principles discussed will show that some principles come up for several authors, while others appear only in the work of one (Table 1). There would not be this discrepancy had these authors appealed to the just war tradition. This contains all of the principles listed and misses none of them out. Furthermore, the just war tradition does not introduce any irrelevant considerations as regards surveillance, once the principles it offers have been applied correctly. Yet an appeal to the just war tradition goes further than this. The tradition has generated considerable philosophical discourse in the last 2,000 years. This rich seam of debate can be mined for considerable benefit in the discussion surrounding the ethics of surveillance.

Consideration	Lyon	Sewell & Barker	RIPA	Kleinig	Marx	Allen	Just War Tradition
Cause	✓	✓	✓	✓	✓	✓	✓
Authority	✓	✓	✓		✓		✓
Intention					✓		✓
Necessity		✓	✓	✓	✓		✓
Chance of Success				✓	✓		✓
Declaration of Intent					✓		✓
Proportionality	✓		✓	✓	✓	✓	✓
Discrimination			✓				✓

Table 1: Summary of Principles Applied to Ethics of Surveillance

I therefore argue in this thesis that the just war tradition provides the most complete framework of questions regarding the ethics of surveillance. Developed over centuries, this tradition deals with the need to limit the harms of warfare, and does so in ways that address issues reminiscent of those raised above. There is a similar distinction between the decision to act (*jus ad bellum*) and the manner in which that action is completed (*jus in bello*); questions are raised concerning the proper authority to act, the justifying cause for the action, the proportionality of that action to the initial situation, and so on. Through appealing to the just war tradition I will show that not only can we address all the questions raised by the authors mentioned above, but we will also avoid missing crucial issues which, as we have seen, are often left out.

2.2 *Jus ad Speculandum*: the Decision to Employ Surveillance

The just war tradition traditionally includes seven principles under *jus ad bellum*: just cause, correct intention, proper authority, last resort, formal declaration, chance of success

and proportionality. If we take these in turn and apply them to the issue of surveillance, the first issue that arises is one of just cause: the reason for the declaration of war and the importance that this be justifiable, usually in terms of defence (either of land or of people and their rights). As with war, and although it might seem obvious to state it, surveillance similarly should not be undertaken for salacious, trivial or ignoble causes (such as protection of pride or of individuals in government, etc.).

So what would count as a just cause for surveillance? This is the subject of chapter 4. Considering the duty of the state to protect its citizens then such activity for the defence of the lives of those citizens would seem to meet this condition. However, states have also found uses for surveillance other than public security, such as identifying political dissidents, which many would not consider justifiable.

At the level of the family, Allen suggests that parental surveillance of children is justified (Allen 2008). She quotes the examples of the parents of the killers at Columbine High School knowing nothing about their children's maintaining arms caches in their homes, and of monitoring the behaviour of children who may become seriously overweight. Yet in these cases Allen overlooks the questions of guilt and warranted suspicion. She thus appears to suggest that *all* parents should be monitoring their children *ceaselessly* lest they too become serial killers at school, which seems to me to be extreme. This raises questions of necessity which shall be considered in due course, but for the purposes of adherence to the principle of just cause, the question is: *are there reasonable grounds for suspicion?* If yes, then it would appear as if a parent would have just cause to closely monitor their child's behaviour. Further to the need for grounds for suspicion is a sense of proportionality to the suspected problem, which I shall also consider shortly.

Between the extremes the macro end of the scale, e.g. the state acting to protect the lives of its citizens, and the micro end, e.g. parents acting to protect their children from going astray, lie a series of different scenarios requiring clarification. Allen looks at the case of Hewlett Packard monitoring the phone conversations of its employees in order to discover a leak (Allen 2008). Is corporate surveillance of employees in the event of a leak a justifying cause? Certainly it is in the interests of the *company* to maintain confidentiality and prevent leaks. Providing that those leaks are of purely commercial interests (that is, they are not the work of a whistle-blower regarding malpractice) then it would seem as if the

company does have *some* justification, insofar as just cause is concerned, in acting to protect that confidentiality through monitoring its employees. However, to what extent the company is justified in carrying out surveillance is a thornier issue. This is especially so when one considers the harms involved in monitoring the conversations of a large number of innocent people, including personal calls to physicians, banks, spouses, etc. in order to apprehend the one guilty employee.

Here a further value of the just war tradition as model in its application to the ethics of surveillance becomes apparent: just because an act may be justified in one respect (in this case, justifying cause), that does not render the act as justified *in toto*. The further considerations of authority, proportionality, likelihood of success, etc. must also be taken into account. While Hewlett Packard may have had a justified cause to conduct surveillance in order to discover a commercial leak, if it had placed its entire workforce under surveillance then this may have been a disproportionate response and so the overall act of surveillance may still not be justified.

The second principle in the just war tradition is correct intention. The intention behind declaring war should be the same as the cause given for going to war, hence preventing ulterior motives from becoming the motivating factor for that war. The moral relevance of intention has been challenged in recent years by philosophers such as Thomas Scanlon. Scanlon argues that intention may be relevant in assessing the moral nature of the decision made by a particular actor, but has nothing to say regarding the moral justification of the act itself (Scanlon 2008). This is in stark contrast to the traditional just war interpretation, which I shall defend in chapter 5.

Intuitively it seems right that intention should be a consideration in assessing surveillance. Firstly, without considering intention it is easy to undermine a just cause requirement by claiming a just cause and using it as a smokescreen for an ulterior motive. Secondly, there is a strong reaction in most people to the difference between, say, a CCTV operator who watches people in the public square to identify known or potential terrorists, and one who watches the same people to identify attractive members of the opposite sex for his own titillation.

The third principle of the just war tradition involves the issue of who is doing the surveillance, and on behalf of whom are they doing it. Traditional just war tradition has tended to hold that the only authority ethically justified in declaring war is the sovereign. Similarly, in the context of genuine national security, the state might be seen to be the proper authority to carry out surveillance on behalf of its citizens. Whether or not the sovereign itself is a legitimate entity, though, is another question. Certainly, if a sovereign loses the moral authority to govern then any potential legitimacy as surveillant *qua* sovereign may also be lost. However, I am not attempting here to extend the analogy to endorse *the same answer* as provided by just war tradition, still less attempting to suggest that the state is the *only* body justified in carrying out surveillance. My point is rather that the question of the moral legitimacy of the surveillant is an issue of major importance that should be addressed when considering the ethics of surveillance.

There are numerous bodies which might claim, or seek to claim, the moral right to conduct surveillance. These include the state, but also the press, corporations, private investigators and individuals. As noted above, one might be hesitant to grant legitimacy of authority to the state purely on the grounds of its being the state, for this overlooks questions of the state's own legitimacy as sovereign. In cases where the governing party has assumed totalitarian control it may see surveillance as a tool for its own survival and so use it against its citizens to discover political dissidents. This might contravene just cause (there is no threat to the state *per se*), but the scenario is such that the authority of the state should also be brought into question. That said, if anyone is to have the moral authority to countenance surveillance, the claims of the state are, under usual circumstances, considerable: the duty of the state to protect its citizens is enshrined in most constitutions, and surveillance may be an effective way to contribute to public security. Furthermore, the mere fear of corruption or totalitarianism should not be allowed to override the need to protect the public. Hence the question of the moral legitimacy of the state to conduct surveillance should be related to the question of the moral legitimacy of the state itself, coupled with the likelihood and extent of possible corruption within a morally legitimate state.

Beyond the state, the legitimacy of non-state actors should also be questioned. If and when the state is a morally legitimate authority in this area, can that legitimacy be conferred upon others such as private surveillance companies carrying out the state's mandate? Are there

other entities such as the free press which can claim moral legitimacy independent of the state? In the latter instance the moral legitimacy of the press might be seen to increase as that of the state decreases in order to continue to provide accountability. Once again, though, the other principles of the tradition should be brought to bear: what is the purpose of the surveillance, is it proportionate, etc. It would be too easy to confer automatic legitimacy insofar as authority is concerned to the press and in the process place the *paparazzi* on a moral plane with investigative political journalism.

At the individual level there is the example of Glenn Michael, as discussed by Allen (Allen 2008). Michael monitored the behaviour of his ex-wife and her suspected lesbian lover in order to gain evidence of her homosexuality which he believed would compromise her custody of their child When brought before a court, the judge agreed with Michael's claim that the child's interests would be better served through being raised by a single heterosexual man rather than two homosexual women. While this is a controversial case, it should be borne in mind that, whatever one's response to the motivation and judgement, in this instance our concern is in relation to the question of legitimate authority. Michael was carrying out the surveillance on behalf of himself (or, arguably, the child). Was he a legitimate authority? Merely being an interested party should not automatically give one the authority to carry out surveillance. Aside from questions of competence, it would be extreme to allow everyone to claim the authority to spy on anyone else in whom they had an interest. Regardless of specific concerns in the Michael case, the legitimacy of the surveillant should be addressed.

Alternatively, Michael might have gone to a private investigator. If such businesses are legitimate within (and regulated by) a morally legitimate state then it is conceivable that the authority of the state to carry out surveillance may be transferred in particular instances to such entities. Hence non-state actors might be legitimate surveillants if legitimacy is conferred by a recognized authority.

An obvious concern with surveillants is whether they are ethically trustworthy in how they gather, store and use their information (both relevant and extraneous). Such concerns can be tempered by state regulation, but in the absence of any regulation then the authority of the surveillant must be called into question, whether legitimated by the state or not. The issue of authority in surveillance will be tackled in chapter 6.

A fourth principle of *jus ad bellum* is last resort, or necessity: that the decision to go to war must come after all other options have been exhausted. Precisely what is meant by last resort in this case is debatable: at which point has a state reached "the final straw" (Walzer 2004, pp.53–54, 88; Lango 2006)? Was it when the Nazis remilitarized the Rhineland? When they annexed Austria? When they invaded Czechoslovakia? When they invaded Poland? When they launched an air invasion of the UK? Or when their allies invaded the US? Furthermore, if the demarche of an ambassador is all that precedes a war then the war might be felt to be somewhat hasty, but if one has to wait until enemy boots are on home soil then this might be leaving it somewhat late. Yet the more one escalates diplomatic and economic sanctions, the more the "enemy" is going to suspect that military sanctions will at some stage follow, and so prepare for defence. Such preparations could lead to a more drawn out and bloody conflict than might otherwise have been the case.

If the question of last resort is debated in relation to going to war, it is similarly unclear in the case of surveillance. Allen takes it as a given that surveillance should have been a last resort in the cases of Michael and Hewlett Packard, and takes it for granted that on neither occasion was this the case. In both instances there were alternatives that should have been attempted. Not knowing the full details of each situation makes it hard to comment directly on Allen's claim, but in the case of covert surveillance with the aim of gathering information the nature of the operation as essentially secretive must surely be relevant. If the surveillance weren't secretive it would risk altering the behaviour of the surveilled. This is, after all, the motivation behind deterrence. Had Michael asked his ex-wife whether she had taken a lesbian lover, and suggested the sanction that if she had he would challenge her custody of their child, then she might have been more careful about closing the curtains at night and so prevented him gaining the necessary evidence for his case. Similar things may be said about the Hewlett Packard case.

Hence if surveillance were truly a final resort it would in many cases be rendered ineffective through losing the aspect of secrecy. In these circumstances it is unlikely to be justifiable as a matter of first resort as there are likely to be less harmful methods which could be attempted. When these have been tried and failed, and they will be different in different scenarios, then the surveillance meets this condition. However, we should also acknowledge that there are some methods which, although less intrusive, could

compromise the later option of covert surveillance. Necessity and surveillance is the topic for chapter 7.

The question of prejudicing results arises again with the fifth principle regarding a formal declaration of war, which we might take in this instance to be a declaration of intent to carry out surveillance. Clearly a formal declaration to carry out surveillance may be inappropriate in the case of covert surveillance lest it alter the behaviour of the surveilled and serve to counter any benefits which might otherwise result from the surveillance. By contrast, in cases of surveillance for deterrence, this would be a good thing, such as indicating the positioning of speed cameras and painting them yellow so that people are aware of them at accident hot spots. The significance of formal declarations might therefore be a problem for justifying particular covert surveillance operations, although less so for the existence of the organisations which conduct those operations. The existence of such organisations can provide a deterrent without giving details of their methods and so compromising actual operations. Formal declaration will be discussed in chapter 8.

The sixth principle is that the war must have a reasonable chance of success, which draws again on the purpose of the surveillance. If surveillance for information is unlikely to return the desired information then that operation is unlikely to be justified. Any information gained will be extraneous, potentially salacious, and bring into question the just cause of the operation. Similarly, if surveillance is justified by reference to deterring crime, and yet actually fails to do this, as UK figures suggest is the case (Hope 2009; Hope 2010), then the justification for its application must once more be brought into question. Reasonable chance of success is an area for which surveillance operations by the state are frequently criticised, as shall be seen in chapter 9.

The seventh and final principle of *jus ad speculandum* has been referred to several times, namely that the projected damage must be proportionate to the occasioning cause. That is, the foreseeable damage that surveillance could incur must be in proportion to the reason by which the surveillance is justified. However, what is meant by proportionality is not always clear. Intuitively many recognize acts as being disproportionate, but determining which considerations should be weighed in the balance in arriving at a conclusion regarding the proportionality of an act is not straightforward. This aspect of proportionality is the topic under discussion in chapter 10.

2.3 *Jus in Speculando*: the Means of Surveillance

The above principles characterize the traditional approach to *jus ad bellum*. Turning to *jus in bello* there are between two and four principles. Most, if not all, agree that proportionality and the principle of discrimination are essential features of *jus in bello*. However, a case is sometimes made for including the further principles of no means *mala in se* and the benevolent treatment of prisoners (Orend 2005). Owing to this distinction, I shall concentrate in this thesis on the principles of proportionality and discrimination in chapters 11 and 12 respectively. It is interesting to speculate as to whether there may be, as Kleinig suggests, acts of surveillance which would class as being *mala in se*, which should never be used (Kleinig 2009)? Without delving too far into science fiction, could mind reading be considered in this category? As to the treatment of prisoners, it could be asked whether those deserving to be subject to surveillance thereby lose all rights to privacy and similar considerations. However, these minor principles do not provide fundamental insights into just war, but rather shortcuts to conclusions reached by the other principles. Means which are regarded as *mala in se*, for example, are typically taken to be such because they are indiscriminate in causing harm or inhumane in the nature of the harm they cause (i.e. disproportionately harmful). Those weapons regarded as *mala in se* would therefore be rejected from use on the basis of other *jus in bello* principles, even if there were no strict principle of *mala in se*. The treatment of prisoners, at least in a general sense, could similarly be derived from considerations of *jus in bello* proportionality. As such I will not consider these minor principles in this thesis.

The principle of proportionality, as with its counterpart in *jus ad bellum*, seeks a response that is proportionate to the occasion. For *jus in bello* application this is less a question of the act of war as proportionate, as of individual actions. Hence the use of tactical nuclear weapons would most likely be judged disproportionate in response to an opponent armed only with rifles, but not an enemy also equipped with nuclear weapons. Applied to surveillance this principle makes a clear reference to the different kinds of surveillance discussed above, and the thought that the less extreme the occasion, the less invasive and pervasive the surveillance should be. CCTV cameras in areas where cars are frequently stolen is more proportionate than bugging the telephones of everyone in the city in which the cars are being stolen. Hacking into an e-mail account to catch an employee suspected

of stealing paper clips seems less justified than doing the same to catch a foreign spy. The principle is thus helpful in assessing which means of surveillance may be employed *in situ*, and so forms a crucial aspect of the ethical framework that must be considered in deploying surveillance. Films such as *Enemy of the State* (Scott 1998) play off this concern when the protagonist finds the full might of the US state surveillance apparatus turned on just one person, the disproportionality of the situation (the use of technology designed to monitor the activities of enemy states being used on a single, and in the event, innocent person) feeding the audience's support for the hero. Proportionality from the perspective of the method of (as opposed to the decision to engage in) surveillance is the subject of chapter 11.

The second *in speculando* principle is that of discrimination: the idea that, in the just war tradition, non-combatants are immune from attack. Clearly there are no strict combatants in most cases of surveillance, unless one is talking about surveillance of enemy troops during times of war, but this principle is nonetheless significant, albeit with some modification. Michael Walzer argues that in everyday life we have a right to life which includes the right not to be attacked (Walzer 2006a pp. 144–45). In the act of donning a uniform and picking up a gun one forfeits that right at the same time as gaining others, such as the manner of treatment if captured. Hence there is an important distinction between those actively involved in the prosecution of the war (combatants) and those not actively involved (non-combatants). As such, one is justified in targeting combatants, who have forfeited their right to immunity, but not non-combatants who retain that right.

If this principle is taken to concern not combatants and non-combatants but legitimate and illegitimate targets, the principle's applicability to surveillance becomes clearer. This is the subject of chapter 12. In the context of security and responding to crime legitimate targets would be those guilty of threatening security or of criminal acts, and illegitimate targets those who are innocent of such acts. An initial response here might be that surveillance should be targeted towards the guilty and away from the innocent as much as possible. However, there is an obvious difficulty here. Surveillance is often carried out in order to *determine* innocence or guilt, and so the status of the surveilled prior to the act of surveillance is frequently unknown. This is a major oversight of Allen who holds that criminals waive some, if not all, of their privacy rights by virtue of having committed a

crime. Yet someone who is wrongly suspected of committing a crime has not waived any rights and so should not be considered a legitimate target for surveillance. This introduces the dilemma that the legitimacy of the surveillance may only be found subsequent to, and dependent on, that surveillance. Prior to the surveillance operation, as far as the surveillant is concerned, the person to be surveilled may or may not be a legitimate target. If they are legitimate then the surveillance is justified, but if they are illegitimate then it is not. As their legitimacy as a target is unknown, the matter of justification appears to be broadly a matter of luck.

In suggesting the possibility of luck, though, one must be careful not to overlook the issue of pre-existent evidence. It has already been established that the decision to carry out the surveillance should not be capricious but resultant on weighing up the likelihood of its success. The justification might come down to the evidence available to the surveillant prior to the decision being made to initiate the operation. The justification for the decision whether to carry out surveillance would then be based on the evidence available rather than the outcome of the surveillance (Lawlor 2006). As such, if the surveilled turned out not to have been guilty, but the evidence that they were guilty prior to the surveillance was strong, then there would have been no miscarriage of justice. On the other hand, if there were no evidence for a person's guilt but surveillance was undertaken anyway then this would appear to be a clear breach of the principle of discrimination, regardless of the result.

2.4 Conclusion

The just war tradition hence provides a powerful framework in which to establish the rights and wrongs of surveillance. The decision to carry out the surveillance is clearly distinct from the methods employed, and each has its own ethical criteria. In deciding whether or not surveillance is justifiable we need to consider who is conducting the operation, what justifications they have given for doing it and whether they have any ulterior motives; whether other, less harmful measures are a plausible alternative; if the surveillance has been declared; whether the operation is likely to be successful; and whether surveillance is proportionate to the occasioning cause. Beyond these are the further issues in the methodology of the surveillance: are the methods employed proportionate to the goal desired; and has the surveillant acted to limit surveillance of illegitimate targets.

These nine principles form an ethical framework for surveillance, grounded in a rich philosophical tradition. As we have seen, they encompass the ethical principles of Lyon, Barker and Sewell, Allen, and Marx but do so in a more coherent and/or comprehensive manner than any of these authors has so far suggested. It also ensures that ethical concerns are not overlooked. This was noted in the way in which Allen does not consider the possibility that a person under surveillance may be innocent and hence not have waived any privacy rights. Similarly, Lyon, Barker and Sewell only suggest tentative principles, none of which consider intention, formal declaration, chance of success or discrimination. With the exception of Allen, neither do they take into account the justification of methodology (*jus in speculando*) as distinct from the decision to employ surveillance (*jus ad speculandum*). Marx is different here as his 29 principles are extremely thorough. However, this list lacks a coherence which can be achieved through appeal to the just war tradition, at the same time tapping into the heritage in moral discourse offered by that tradition. This discourse holds a huge literature of value to this debate, much of which will prove to be directly applicable.

Hence the just war tradition can indeed be used to assess justifications for surveillance operations. Furthermore it *should* be used in that it adequately captures the concerns of those writing in this field and helps us to take into consideration legitimate concerns which are often missed by others.

3. The Benefits and Harms of Surveillance

This chapter outlines the most plausible benefits and harms that arise from surveillance. It is likely that no one act of surveillance will include all of these. Monitoring what school children buy for their lunch, for instance, is unlikely to instil a sense of social fatalism among those children. I shall assume that all instances of surveillance discussed are non-consenting.

It should be noted that there is remarkably little reliable empirical evidence for any harms or benefits, largely because this is so difficult to obtain. Take for instance the risk of chilling effects. Chilling effects, the fear from engaging in legitimate activities due to a fear of being singled out and harmed for this engagement, were first recognized by the US Supreme Court in *Weiman vs. Updegraff* (1952, see Columbia Law Review 1969). One of the best examples of the chilling effects of surveillance is the former German Democratic Republic (GDR), in which a vast number of citizens were employed to inform on their neighbours and dissidents were regularly imprisoned, tortured and killed. It is noteworthy how few public demonstrations against the government there were in the GDR, arguably as a result of this chill. However, it is virtually impossible to determine how much of the chill was due to the surveillance and how much to the imprisonments, etc. If, for instance, the Stasi (secret police) in the GDR had maintained the same level of surveillance but only interfered in the case of domestic accidents which required a sticking plaster, bandage or potential hospitalization, and then if the interference was entirely benign, it is difficult to say whether there would still have been chilling effects from the surveillance.

One way to avoid this problem of isolating cause and effect is to refer to the system rather than the act which forms a part of that system. A system in surveillance is therefore the entire package: not just the surveillance itself but also the surveilled subject, the surveillant and the society they both inhabit. Hence the surveillance system of the Stasi caused a chilling effect, but whether it was the surveillance or the consequences of the surveillance is less important. More important from this perspective is that, with the possible exception of God, there has never been, and probably never will be, a “benign Stasi” such as I have described.

From the perspective of conceptual analysis, though, any refusal to explore the individual acts which together comprise a system will be unsatisfying. It is not surprising that surveillance + secret police + imprisonment + torture + death = chilling effect. In writing a study on surveillance *per se*, though, it is desirable to remove these elements until only the surveillance and its effects remain. Even if the surveillance is not a direct contributing factor to harms such as chill, it may *enable* the larger apparatus which in turn creates that chill. As a significant enabler of harms, then, it is important to note that such surveillance can still be harmful.

In the absence of any controlled experiments, or counter-examples, it must be accepted that any account of the benefits and harms of surveillance must be, to a degree, speculative and appeal to the reader's intuitive sense of plausibility rather than empirically-obtained data. This chapter is therefore intended to bring a philosophical approach to a predominantly sociological discussion. Hence while it is acceptable practice to discuss surveillance as a system, in this chapter I separate out the different harms and benefits that plausibly arise from acts of surveillance.

A final introductory point is that surveillance is often viewed as an aspect of individual concern. It is the individual's privacy which is threatened, an individual who is at risk of being "found out". It is similarly the individual whose journey time through the security queue at an airport is reduced by the implementation of better security scanning techniques, and who feels safer walking through a town centre at night knowing that there are CCTV cameras watching her lest she be attacked.

However, the benefits and harms of surveillance are not restricted to individuals. There are social implications as well. These are illustrated in Orwell's *1984* or the GDR once again (the foregoing points accepted) as society becomes more bland and fatalistic. Creativity is stymied and social discrimination can abound in unseen ways. Because of these considerations I have, somewhat artificially, separated the benefits and harms into categories of social and individual. It is an artificial dichotomy as few if any individuals who are subject to surveillance exist outside a society, and society is ultimately made up of individuals. The distinction is more one of perspective than of type. Nonetheless, through this perspective I shall demonstrate that the benefits and harms can be seen to affect the individual and society in different ways.

In this distinction I am not advocating a clash of individual versus society in which one is seen as being more important than the other. While an important debate, that is not what I seek to achieve here. Rather, some harms are more relevant to society than to individuals, while others affect individuals more. In the case of society the fundamental questions are what sort of society do we value, and what sort of society will surveillance produce. From the individual perspective the fundamental question is more a matter of how is surveillance likely to impact the well-being, rights and interests of the individual. The harms themselves, as I argue below, are not mutually exclusive to either individual or society.

Before looking at the benefits and harms in greater depth, Table 2 presents an overview of those which I shall consider, noting whether they are of predominantly individual or societal concern.

	Benefits	**Harms**
Society	1. Security a. Deterrence b. Prevention c. Detection 2. Efficiency in bureaucracy 3. More effective governance 4. Monitoring infants, children and the mentally handicapped	1. Chilling effects 2. Paternalism 3. Social fatalism 4. Behavioural uniformity 5. Human error and abuse of power 6. Social sorting – stereotyping, stigmatization, discrimination 7. Imbalance of distribution of costs
Individual	1. Security a. Deterrence b. Prevention c. Detection 2. Efficiency 3. Ease of use 4. Faster 5. Personalised service	1. Privacy violations 2. Vulnerability 3. Fear of control 4. Human error and abuse of power 5. Fear of being "found out" when hiding legitimate but not criminal information

Table 2: Benefits and Harms of Surveillance

3.2 Society

3.2.1 Benefits

The benefits to society that arise from surveillance can be significant. At times of perceived threat, the potential that surveillance offers to reduce the risk of that threat occurring can render surveillance attractive. This threat may be natural, in the sense of earthquakes, tsunamis or volcanoes, or it may be human in the sense of crime, terrorism or war. In either case surveillance is employed to give advance warning of the actualization of these threats. In the case of natural threats this is uncontroversial. No-one is concerned at scientists burying seismic indicators near known fault-lines in order to gain advance warning of an earthquake. Indeed, the surveillance of nature is not at issue here for that reason. It is the surveillance of humans that raises particular ethical issues.

In the case of human threats the surveillance has, or could have, an impact on the people coming under that surveillance. Indeed, some surveillance is designed specifically to have an impact on people. Under a general heading of security from human threats come the three aspects of deterrence, prevention, and detection. Deterrence is surveillance that is used in an effort to deter a would-be criminal from engaging in his crime. This may come in the form of notices displaying that CCTV is in operation in this area, warning signs that traffic speed cameras are in use along a certain stretch of road, or letting it be known that police may put wiretaps on the phones of suspected terrorists. In each case there is a desire to alter the behaviour of people who would otherwise engage in some form of wrongdoing.

The second aspect of security here is prevention. Obviously deterrence is a form of prevention, however here is meant prevention when deterrence has failed. That is, surveillance is employed to gain advance notice of a wrongdoing such that the police or security services can intervene before that wrongdoing occurs. Typically this would include acts of terrorism or organised crime. However, with developments in technology, this is increasingly being seen to encompass what has been called “pre-crime”, following the Philip K. Dick short story *Minority Report* (Dick 2000). Pre-crime involves the controversial tracking of suspicious behaviour by individuals with the motive of recognizing criminal intent before a crime occurs. Intervention can then take place to prevent the crime (see Lomell 2012).

The third and final aspect of security here is detection. This occurs after deterrence and prevention have both failed such that a wrongdoing has occurred. In the aftermath of this wrongdoing evidence is gathered, much of which may come from forms of passive surveillance (passive in the sense of continuously recording without any specific purpose other than assistance in the event of crime detection). Hence in the aftermath of a stabbing outside a nightclub, police will typically request CCTV footage from local businesses to see whether the individuals involved can be identified and the motive established. Following the 7 July London bombings in 2005 such footage was used to piece together the practice runs and final few hours of those who were to blow themselves up with such devastating effect.

All three of these aspects of security involve individuals but have a broader social benefit. Without wanting to endorse any one political philosophy, many hold that one of the prime reasons for society existing is through a desire for gained security. As such, the increase in security (or perceived security) is of benefit to the well-being of society as a whole. That is, it is in the interests of all for society to be a secure environment in which individuals can flourish while obeying the laws of that society.

Clearly not all surveillance has a direct impact on security, and some may have no impact at all. A unified national health database can ensure that no matter where a person is in the country, if hospitalised a doctor can retrieve that person's medical history instantly and be aware of any drug intolerance that may affect the treatment given to him. Similarly surveillance on public transport systems can identify choke points in which many people crowd into one area. This can be used to filter users more effectively or assist with restructuring that area to cope with the increased numbers. Hence surveillance can assist in making bureaucracy and governance more efficient and more effective.

A related advantage to improvements in efficiency and efficacy of bureaucracy and governance is the extension of paternalism by the state. This is more controversial as a benefit, and I shall also discuss it as a harm. Nonetheless, surveillance of this nature can enable the state, through accurately knowing its citizens' situation, to take a more active role in providing welfare for its citizens. Nor is this limited to the state. Paternalism can work at a more local level in hospitals and care homes. Here surveillance can oversee the infirm or elderly to ensure that if they get into trouble then help can be provided quickly.

In some care homes pressure pads alert staff when an elderly person has got out of bed in the night, and how many times they have opened the refrigerator door. Each of these can be indicative of their overall fluid intake and retention. Should an anomaly appear in the person's behaviour then staff can quickly intervene.

Monitoring for paternalistic reasons is not limited to the infirm and elderly, though. It also extends to the monitoring of infants. Many parents regularly use baby monitors that broadcast sound and video from a child's room. This enables the parent to intervene quickly should the child wake and cry, and to have piece of mind that the child is safe if gentle, regular breathing can be heard.

Surveillance of children is not limited to the infant years. As children grow in mental and physical capacity, as well as maturity and independence, so they continue to require surveillance to prevent them from encountering harms which they could not reasonably foresee, or harms which they could foresee but did not predict realistically. With younger children this is effected through parental oversight coupled with day care and later schools acting *in loco parentis*. As the child grows into a teenager, more trust will likely be demonstrated by the parents. At the same time, parental forms of monitoring may alter by, for instance, tracking a teenager by the location of his or her phone rather than placing a camera and microphone in that teenager's bedroom. These could be seen to be for the security of the child. For similar security-related reasons many schools now have a "no cash" policy to prevent children being bullied for their lunch money. Instead lunch is paid for from an account which is accessed by the child through a fingerprint scanner. This has the added advantage that parents can then also monitor the food that their child is buying and so have an influence in favour of a healthy lifestyle even when the child is not at home.

In the monitoring of both infants and children there are aspects of security and paternalism. In general paternalism is expected towards a child. It is only problematic when exercised towards an autonomous, mentally competent adult, or inappropriately towards a child (either because the child is too old to be treated in this way, or the person acting paternalistically towards the child lacks the authority to do this) that it becomes problematic. These more controversial aspects of paternalism will be dealt with in chapters 4 and 6 respectively.

3.2.2 Harms

While there are many benefits of surveillance from a social perspective, there can also be harms. In considering the social harms of surveillance one can do worse than look at societies which engage in large-scale surveillance such as the former GDR, the former Soviet Union, North Korea, or China. However, as noted in the introduction, one of the problems in using real examples such as totalitarian states to demonstrate the effects of surveillance is that it is hard to separate those effects from others generated by oppressive living conditions in a totalitarian state. Saying that, it is of course pertinent to note that much of the suppression of political dissent could not have happened without surveillance. As such, although not necessarily harmful in and of itself, in totalitarian regimes surveillance might be the only way to effectively enable repression.

People who have lived through totalitarian regimes often cite the perpetual surveillance itself as being an oppressive element. In her book *Stasiland* Anna Funder quotes one source as saying, "At the time I criticised other things — not being allowed to study or have a career. But looking back on it, *it's the total surveillance that damaged me the worst*. I know how far people will transgress over your boundaries — until you have no private sphere left at all. And I think that is a terrible knowledge to have [emphasis added]" (Funder 2004 p.113).

One of the greatest social impacts of surveillance is the aforementioned chilling effect. People could become fearful of engaging in officially legitimate but unwelcome activities, such as demonstrating or voicing dissent. Such curtailment of democratic practices will have an impact on the nature of that society. It is interesting that the Stasi referred to its surveillance as "Operational Control of Persons" (Funder 2004 p. 198), directly connecting surveillance with social control. Furthermore, this is not limited to state surveillance. Anyone who has lived with nosy neighbours will know the temptation to hide certain goods that they are either bringing into or getting out of the home. Such neighbours may, for example, vociferously disapprove of alcohol. As a result the householder may feel the need to hide any alcoholic beverages that they bring into the house or put out for recycling.

As raised earlier, there is an interesting question here as to whether Funder's interlocutor would have felt the same had the Stasi been benevolent. Would benevolent surveillance

still lead to chilling effects? My suspicion is that even with the best will in the world most people would soon find this stultifying and increasingly destructive of emotional stability. The sense of being watched is not necessarily oppressive in the short term, but over time it could have the cumulative effect of a dripping tap. Furthermore, the mere possibility of there being a connection between the surveillance and malevolent actions by the state may be sufficient for many to experience that surveillance as a harm. As such, without consent to the surveillance I believe that it would (or at least could) become oppressive no matter the motive.

Against the argument that surveillance leads to chilling effects could be posited the fact that there does not appear to have been a decline in social criticism in some heavily-surveilled societies such as the UK, despite the growth in surveillance over the last 20 years (Barrett 2012; Hastings 2012). This, though, could be interpreted variously as a lack of chilling effect or an increase in the bravery of social critics in standing up to the entrenched powers. It may also be that the majority of that surveillance is focussed on petty crime and anti-social behaviour rather than political protest, although political activists do point to clear acts of significant state surveillance of their legitimate activities (O'Hagan 2012). As stated above, though, this is not an empirical study and I leave it to others to confirm or deny these suspicions.

A second social concern with surveillance is that of paternalism when directed at non-consenting, autonomous adults. States maintaining a high degree of surveillance of their citizens may justify this in terms of the citizens' own best interests, possibly couched in the language of ideology to "help" people become better citizens (as in Orwell's *1984*). This degree of paternalism is objectionable on its own grounds. The government, it is argued, is there to provide security for its citizens and little else. Libertarians and liberals alike have argued strenuously against paternalism (e.g. Nozick 2001; Feinberg 1986). A more detailed examination of paternalism, resulting in the conclusion that it is not justified, will be given in Chapter 4. For the present purposes, though, it is sufficient to include paternalism as a plausible harm.

In addition to paternalism, what may start out as a genuine desire to help citizens by making their lives easier can develop into a sense of fatalism in the minds of those citizens. They may come to believe that the state is constantly monitoring and controlling all aspects

of their lives, and that there is nothing they can do without the knowledge or indeed control of the state. Effecting change in the state or even in their own lives could thereby cease to be an option, and so democratic participation or even a desire to change life circumstances can become muted.

A fourth harm is the development of behavioural uniformity. Coupled with chilling effects and social fatalism, there could arise a desire to keep one's head down, to "blend into the crowd". Even where uniforms are not provided to citizens, as in Orwell's *1984* or Mao's China, dress and behaviour may veer away from the creative or the individualistic. This could amount to a suppression of individual autonomy and freedom of expression. Again, this is difficult to assess as a response to surveillance *per se*. In both *1984* and Mao's China uniform was the required (or indeed the only available) dress for the middle classes. Similarly, and following Plato's *Republic*, creative expression was channelled into art that would bolster the state (Plato 2007; Orwell 2004). Hence deviations from uniformity or artistic expression not endorsed by the state were punished. In order to determine the effect of surveillance assessment needs to be made of these areas in which punishment was not threatened.

A fifth harm is human error. This is clearly a potential harm of, rather than one which necessarily follows from, surveillance. Mistakes can be and are made in bureaucratic processes arising from a lack of knowledge about individual people. A person sharing the same name as a paedophile may find they are put on the child abuse register. A simple mistake, this can have obvious devastating effects on a person's life (see, for example, Bond & McDugall 2009; see also Gilliam 1985). On a more extreme scale such "errors" could be deliberate, involving actual abuse. The power of those with access to the information collected by surveillance is thus heightened and entrenched by the lack of democratic accountability. This challenge to democratic accountability stems from either indirect chilling effects or direct democratic suppression.

The final harm that I will consider is "social sorting" (Lyon 2002). This involves the entrenchment and exacerbation of social differences through the use of surveillance. David Lyon has argued that surveillance is frequently used, wittingly or not, to stereotype, discriminate, and stigmatise groups within society. From the use of customer loyalty cards to automated payment on toll roads, surveillance systems create, develop or entrench

differences within society. This is perhaps more ambiguous than other harms. For instance, it may not be morally problematic if the people identified by the surveillance and stigmatised as a result are all and only active criminals (Macnish 2012). However, insofar as surveillance serves to discriminate unfairly (although what one counts as unfair may be less clear) then this is clearly problematic.

Related to recognizing the harm of social sorting is an awareness that harms typically do not fall equally across all members of society. Hence it may be that a non-Islamic society as a whole wishes to feel safer in the wake of an Islamic-inspired terrorist incident and so that society condones the profiling of Muslims and those believed likely to be sympathetic to Islamic terrorism based on ethnic background. Presuming that the profiled category falls into the minority then society as a whole may feel safer at the same time as that minority unjustly suffers harassment and stigmatization. This problem of profiling is an important point which is worth developing in greater detail.

3.2.2.1 Group Profiling[2]

3.2.2.1.1 Group Profiling in Theory

There are two main concerns with profiling based on membership of a group: unjustified stigmatization and harassment of the innocent. These can be illustrated across four scenarios which, using teenagers and shoplifting as an arbitrary example, contrast the hypothetical situation between every teenager shoplifting, only teenagers shoplifting, some teenagers shoplifting and some non-teenagers shoplifting. The four alternatives are:

i) it is known that every teenager and only teenagers engage in shoplifting;

ii) it is known that every teenager but not only teenagers engage in shoplifting;

iii) it is known that not every teenager but only teenagers engage in shoplifting; and

iv) it is known that not every teenager and not only teenagers engage in shoplifting.

[2] The following is adapted from (Macnish 2012) and is used with permission, licence number 3176401090089.

For the sake of the illustration I will assume that the surveillance is 100% effective and, other things being equal, fully warranted in the case of apprehending shoplifters. I will also assume that the facts regarding teenagers and shoplifting are known in each scenario and that these facts will not change over time. Finally, I will also assume that there is no change over time, so the surveillance has no deterrent effect. For the time being I will leave aside the question as to how different these cases are from reality, although I shall return to this issue at the end of this section.

In scenario (i) it would be unobjectionable to carry out surveillance on teenagers. Given that the surveillance is effective and warranted, then if every teenager shoplifts and no-one who is not a teenager shoplifts profiling would be justified. While it might be argued that this stigmatizes teenagers, it does not do so unjustifiably. They are singled out as shoplifters because they are unique in their shoplifting, and no innocents have been stigmatized.[3]

Scenario (ii) presents a more difficult case: every teenager shoplifts, so focusing attention purely on teenagers would capture all shoplifting teenagers. However not only teenagers shoplift, so older (or younger) shoplifters will go unchallenged. This is perhaps unfair in treating just teenagers as shoplifters when this is not the case. Other members of society also steal from shops and so teenagers are no different in this respect. However the fact remains that all teenagers are shoplifters. The central problem here is how effective such profiling of teenagers would be: it seems important to ask how many non-teenagers shoplift. We might imagine a city, Cleptopolis I (population 10,000) in which there are 2,000 teenagers, all of them shoplifters. However there are 5,000 shoplifters in all. In this case the majority of shoplifters are in fact not teenagers, and so focusing on teenagers would have limited, albeit perhaps significant, impact on reducing shoplifting. To catch the majority of the shoplifters a further policy would need to be put in place, in the absence of which the surveillance would be far from perfect as it fails to catch most shoplifters. It may also transpire that the policy focuses unfairly on teenagers. It is important here to query the composition of the group of 3,000 non-teenage shoplifters. Are they all people in their early-20s, all aged between 70 and 80, or are they a random spread of the non-teenage

[3] This also does not deny that there might be deep-seated reasons for the shoplifting which should be addressed beyond any judicial punishment for the crime following apprehension.

population? If either of the former (and assuming that either of these were easily identifiable) then to focus surveillance solely on teenagers and not the larger group of shoplifters in their early-20s or the septuagenarians would be to stigmatize the teenagers unfairly. Were the majority a random spread of the non-teenage population, though, then there would not be unfair stigmatization.

In neighbouring Cleptopolis II, given the same population and age distribution, the total number of shoplifters is 2,001. There is one adult who could not kick the habit as he passed into his 20s. In Cleptopolis II the scenario appears to be very close to scenario (i) in that every and (almost) only teenagers shoplift. As such an exclusive focus on teenagers in Cleptopolis II would be more justifiable than in Cleptopolis I, given that such a focus would miss only one shoplifter in Cleptopolis II whereas it would miss 3,000 (the majority) in Cleptopolis I. As noted above, it would depend on the composition of the majority in Cleptopolis I as to whether there were unjust stigmatization of teenagers. Assuming that the majority were a random spread of the non-teenage population, though, in neither case are teenagers being stigmatized unjustifiably nor are the innocent being harassed.

Scenario (iii) envisages the situation in which it is known that only teenagers engage in shoplifting. It is also known that not all teenagers are shoplifters. In this case focusing surveillance on teenagers does lead to unjustified stigmatization and harassment of the innocent. The innocent may see themselves as being treated as if guilty, lumped in with the genuinely guilty simply because of their age. They are treated with suspicion owing to the actions of a number of others in their group. They might not know the others or have any influence over their actions. Nonetheless they suffer the consequences of those actions through no fault of their own. It may be argued, though, that it is not teenagers that are being targeted. Rather, we start with the presumption that everyone should be targeted but then those groups *known* to be innocent are *excluded* from targeting. It just so happens that after all other groups are excluded, the only group left is teenagers. While this may seem like cynical word-play (after all the effect is the same) it demonstrates the importance of perceptions in understanding stigmatization. That is, there may genuinely be no intention to stigmatize, but the result might be such that those affected by the decision feel stigmatized nonetheless.

As with scenario (ii) there will, in scenario (iii), be a question of how many of the innocent will feel stigmatized and harassed. Imagine Diebesstadt I and II, cities of identical population and age distribution to Cleptopolis I and II. In Diebesstadt I there are 1,100 shoplifters, all of whom are teenagers. By focussing surveillance on teenagers there are then 900 innocent teenagers who are treated as suspicious and harassed unjustifiably. In Diebesstadt II, however, of the 2,000 teenagers 1,999 of them are shoplifters. In this case there is just one teenager who is innocent. The numbers make Diebesstadt II very close to scenario (i) as (almost) every and only teenagers shoplift. The consideration of surveillance of teenagers in Diebesstadt II then turns on the importance placed on the harm visited on the one innocent.

Finally there is scenario (iv) in which not every teenager and not only teenagers steal from shops. Of the four this is the only case which exists in the real world. If targeting teenagers when not only teenagers shoplift leads to ineffective surveillance, and targeting teenagers when not all teenagers shoplift both stigmatizes and harasses the innocent, then in scenario (iv) such targeting risks both ineffective surveillance and the stigmatization and harassment of the innocent. As with scenarios (ii) and (iii), the numbers here also matter. The closer the numbers approach scenario (i) of every and only teenagers shoplifting the more effective will be the surveillance, the more justifiable will be the stigmatization and the fewer innocents harassed. By contrast as the numbers involved fall to levels of many, some or just a few teenagers shoplifting, so these concerns become more problematic and less justifiable. As above, much of the justification will turn on the importance placed on the harm visited on the innocents, especially when weighed against society's desire to be free from shoplifting.

A final problem is that the above scenarios are hypothetical and not realistic. It is rarely the case that only one group engages in acts of wrongdoing, still rarer that that group is easily identifiable, and rarer still that authorities carrying out surveillance know that all, some or none of the group are involved. More realistic versions of scenarios (i-iv) are also unlikely to remain static over time. Even if scenario (i) were to exist in a particular city for a particular year, the following year the statistics may change such that scenario (iii) now prevails. Hence in one year a policy such as that suggested above may be devised involving the justified stigmatization of teenagers, owing to the fact that they are all known

to shoplift. In a subsequent year, in which the individuals making up the population of teenagers has changed such that not all teenagers now shoplift, the policy would involve the *un*justified stigmatization of teenagers. The change in the justification of the policy would have nothing to do with the policy *per se*, but rather changes in the group it is singling out for attention. Finally, the consequences of any perceived stigmatization might be that more teenagers begin to shoplift (thinking that they will be treated as shoplifters either way). As such the unjustified stigmatization might serve to encourage shoplifting over time, rather than reduce it.

In summary I have argued that there are four alternative scenarios with reference to teenagers and shoplifting:

i) every teenager and only teenagers engage in shoplifting;

ii) every teenager but not only teenagers engage in shoplifting;

iii) not every teenager but only teenagers engage in shoplifting; and

iv) not every teenager and not only teenagers engage in shoplifting.

Of these, scenario (i) was seen to be unproblematic in terms of stigmatization and harassment of the innocent. That is, in cases where every teenager engages in shoplifting the profiling of such teenagers does not lead to these harms. Depending on the numbers and composition of non-teenage shoplifters in scenario (ii) the profiling may prove to be inefficient, in that it could fail to identify the majority of shoplifters and potentially be stigmatizing. Scenarios (iii) and (iv) were seen to demonstrate unjustified stigmatization and harassment of the innocent. It was notable that this could be the case, at least in the perception of some, even where no stigmatization was intended. In such cases considerable effort needs to be extended to explaining the justification for the surveillance such that the intention is clear. Even then, it may be that the unintentional stigmatization is such (or to such an extent) that the surveillance cannot be justified. Finally, the levels of knowledge and the composition of the groups assumed in the hypothetical cases are unrealistic, and changes may occur between the scenarios over time, such that a policy which was at one time justified may become unjustified, and would need to be altered accordingly.

3.2.2.1.2 Group Profiling in Reality

The above cases of Cleptopolis and Diebesstadt are unrealistic and overly simplistic, yet they clarify major problems with profiling based on group membership. In more realistic cases when the numbers are far less extreme and when change and fallibility are introduced into the scenario these problems will be exacerbated. Furthermore, surveillance is rarely if ever 100% effective and it might not be warranted in particular cases. One might think here of the surveillance of dog walkers to apprehend those who do not clean up after their animal has defecated (Slack 2010). Such cases are typically dismissed as being disproportionate when weighing the potential harms involved and the benefits gained, as well as challenging the perceived interests of individuals to walk freely without state interference.

In addition to these concerns, there is a further issue of self-fulfilling prophecies. Through watching teenagers more closely, more shoplifting teenagers will be caught stealing and sentenced. As more teenagers are sentenced for shoplifting, so the statistics will show that a disproportionate number of shoplifters are teenagers. This will then justify the further concentration of attention on teenagers and so on. Meanwhile, other (non-teenage) shoplifters could continue to go undetected by the surveillance which increasingly ignores them. Those who stigmatize teenagers might then feel affirmed in their prejudice and continue to indulge it.

Identification of threat based on group identity is therefore likely to be problematic in most real-life cases. It introduces or perpetuates stigmatization, places a burden of suspicion on the innocent and risks instituting self-fulfilling prophecies. Furthermore such group identification is rarely limited to particular age groups, as in the above examples. It often includes ethnicity and religious identification, especially when related to crime and particularly terrorism (Warikoo 2011). As a result it seems as if there should be a presumption against group profiling unless it can be demonstrated that a) a significant majority of the group deserve to be subjected to surveillance (although quite how many form a “significant majority” is unclear); b) the ensuing wrongs outlined above are outweighed by competing considerations among the benefits to be had from the surveillance, such as security; and c) the surveillance is both effective and warranted in the particular case.

3.2.2.2 Behavioural Profiling

What then of identifying threats according to behaviour? Were the target group to act in a distinctive way then they could again be singled out for attention while the majority are unaffected. However, such distinctive behaviours seem hard to find. When operators and the police have restricted their attention to "suspicious behaviour", this concept has often been ill-defined and of limited value, including behaviours such as running in a public place or covering the face (Norris & Armstrong 1999; Graham 1998; PACE 1984). While these are potentially suspicious activities, the running may be to catch a bus and the covering of the face a reaction to cold weather. Context needs to be taken into consideration in such cases. Related problems have been noted in police "stop and search" tactics which require "reasonable grounds for suspicion". In practice these evince a high degree of prejudice against particular age groups and ethnicities (Dodd 2010). This may be because these groups display behaviour which is misinterpreted as suspicious by police, particularly when the police are predominantly drawn from a different age or ethnicity. However it may also be due to the poor definition of "suspicious" meaning that behavioural profiling can serve as a mask for continued group profiling. As such the problems of prejudice once more come to the fore.

Even when it is not masking group prejudice *per se*, behavioural profiling can still involve prejudice. As noted above, different age and socio-ethnic groups are known to display different behavioural characteristics. One only has to think of the difficulty many adults have in communicating with teenagers to realise that what is normal behaviour in one age group can be abnormal in another. By defining a particular behaviour or characteristic as identifying a threat, there is a risk that one also inadvertently identifies an innocent group which uses that behaviour in a non-threatening manner. Consider here large groups of teenagers hanging around outside McDonalds with their hoods up and their heads bent. For many adults this carries a lurking sense of threat, even when no threat is intended on the part of the teenagers.

More directly, the behaviour could be that which identifies a group. Not all teenagers wear their hoods up, and so the wearing of a hood will not be sufficient to identify all members of a group. However, it might be that all members of a particular group perform a

particular action such as attending a synagogue on Saturdays. As such the behaviour might be that which is explicitly profiled, but the effect would be the same as in group profiling.

3.2.3 Summary

The potential social harms of surveillance are therefore considerable. The central concern might best be summarised as an infringement on democratic principles. This is the impact of chilling effects, paternalism, social fatalism, and behavioural uniformity. Beyond the impact on democracy, though, there is the risk of a pervasive sense of fear arising from a disproportionate amount of information and control held by those in power. The temptations for abuse of that information may be great, and the scope for accountability low or non-existent. Finally, surveillance is often unfairly discriminatory, and this discrimination can have negative impacts on sectors of society, leading to unjust stigmatization or harassment of the innocent.

3.3 Individual

3.3.1 Benefits

As there are potential benefits and potential harms which accrue to society as a result of surveillance, so too are there potential benefits and potential harms which accrue to individuals. In some ways these may be more obvious than the societal impacts and so I have chosen to list these second in order to raise the profile of the former.

An obvious benefit to accrue to the individual from surveillance is, as with society, security in the form of deterrence, prevention and detection. Through the individual's own vigilance he can do much to ensure his own safety, and in many cases simply being vigilant can deter others from an attempted mugging or other attack (Navarro 2012). Similarly, surveillance of one's neighbourhood by groups such as Neighbourhood Watch can bring to light people who are acting suspiciously and may be intending to commit some act of wrongdoing. Finally, in the event of a break-in a homeowner with CCTV may be able to use footage recorded by the camera to assist in the detection of the burglar.

Following from the societal benefits of efficiency and efficacy which accrue to bureaucracies and governance, the individual can similarly benefit from these in terms of

his own efficiency (not having to wait for hours when dealing with local government as they have a record of precisely who he is and where he lives); he may have less hassle in dealing with these institutions through being able to prove who he is more easily, and finally his progress through institutionalised processes is likely to be faster as a result of these. Indeed, the reason why people choose to surrender their privacy to the state in voluntary schemes is often in order to gain advantages in terms of speed and efficiency when dealing with bureaucracies. The same is true in giving private information to websites in return for services which do not charge fees for their use, such as Facebook.

At a more personal level, John L. Locke argues in his book, *Eavesdropping: an intimate history* that there are benefits for a community which lives with little privacy, such as a greater degree of intimacy and an enhanced sense of community, not to mention accountability (Locke 2010 pp. 71–3). This is taken up by Jeff Jarvis who argues in favour of a life lived publicly (Jarvis 2011). The benefits of such a life, according to Jarvis, include building relationships, disarming strangers, enabling collaboration, unleashing the generosity and wisdom of crowds, defusing the myth of perfection, and neutralizing stigma (Jarvis 2011 pp. 43–62).

A final benefit to be gained for the individual from surveillance is a more personalized service. Nicholas Negroponte has argued that if I must be subject to advertising in return for a notionally free service then at least make the advertising relevant to me (Negroponte 1995 pp. 164–65). Do not show me a high-end luxury car if all that I can afford is a rust bucket from the 1970s. Amazon has taken this philosophy to heart with personalised recommendations based on items that customers have viewed in the past. The detail of these recommendations is beyond what any shop on the high street is able to offer. Supermarkets are also able to deal with massive quantities of data such that they are able to make accurate predictions about the life-circumstances and associated needs and desires of their customers (Duhigg 2012). In both cases these uses of surveillance advantage those who opt-in (or in some cases buy-in) to the system.

3.3.2 Harms

As with benefits to the individual, there will likely be crossovers between societal and individual harms. Hence as surveillance discriminates, so it will be individuals who are

discriminated against. Likewise if surveillance does repress creative expression then people such as artists who live off their creativity (particularly if their art tends to be critical of those empowered and in control of surveillance) could suffer from that form of repression. They might experience harms to their livelihood, to their personality and to their freedom of personal expression. Acknowledging that, and with the earlier proviso that the distinction between societal and individual harms is one of perspective rather than an absolute distinction, I will here concentrate on harms which are more specific to the individual than society.

The most obvious harm to the individual that can arise from surveillance is a violation of privacy. Whether the surveillance takes the form of visual monitoring, aural wiretaps, or Internet records, in each case the purpose of the surveillance is to reveal information which the surveilled might prefer not to have revealed. The surveillance may therefore constitute a violation of the individual's privacy. Privacy is understood to be a right in both Article 12 of the Universal Declaration on Human Rights and in Article 8 of the European Charter of Human Rights (Giacomo 2011; United Nations 1948). This is not to say that it is a moral right, still less one which may trump other rights, nor that it is an absolute right which may never be lost or infringed upon. There are surely cases, as both the Declaration and the Charter recognize, in which privacy can and should be overridden (in the interests of national security, for example). However, it is to recognise that privacy is broadly seen as being a universal good and in the interests of each person.

In addition to its being enshrined as a right in international law, there is strong anthropological evidence for a universal interest in privacy. Even groups which live communally, such as Eskimo families in open plan igloos and the Yagua of north-eastern Peru, still observe some aspects of privacy. They turn away or avert their eyes when a member of the group is "engaged in intimate personal and family activities" (Locke 2010 p. 74). This may not seem like much from a western perspective where we are used to living within walls and having our own bedrooms, but it is nonetheless a rudimentary respect for the privacy of another.

We have good reasons to desire and maintain what privacy we do have, points out Locke (Locke 2010 pp. 86–91). There are certain human activities which, while we all do them, would be demeaning to our dignity were we to be watched whilst doing them. Most of us have locks on our bathroom doors, for instance. There is also the pleasure of solitude, "the freedom to rest, reflect, and enjoy one's own company" (Locke 2010 pp. 88–9). As such it seems fair to say that there is a universal need for privacy, although how this is realised may differ across cultures and indeed across time within a single culture.

In philosophy, most writings on the subject of privacy acknowledge that it is an individual interest. Disagreement typically arises in what is entailed by privacy, and why it should be valuable. Hence Tony Doyle has denied that there is an intrinsic value to privacy (although he accepts an instrumental value) and Judith Jarvis Thomson has argued that privacy is an amalgamation of other rights, particularly property rights, brought together in a particular context (Doyle 2009; Thomson 1975). In contrast to this, Thomas Scanlon has argued that privacy is a distinct right involving zones which enable us to act in the assumption that we are not subject to surveillance (Scanlon 1975). James Rachels presents something similar in his notion of the value of privacy being the means by which relationships are defined (Rachels 1975). He claimed that the relinquishing of privacy to certain people demonstrated that they were more trusted and privy to a more intimate relationship. This has been developed more recently by Helen Nissenbaum (Nissenbaum 2004). Others argue that privacy enables autonomy, the freedom to experiment with ideas and choose freely without fear of the interference of others (Gavison 1984 pp. 363–64; Benn 1971).

A further discussion has developed as to whether privacy involves control or access. If you forcibly take my diary, you have seized control over it from me, and so, according to W.A. Parent, Daniel Nathan and danah boyd, you have violated my privacy (boyd 2010; Nathan 1990; Parent 1983). Others argue that no violation has occurred unless you actually read my diary and gain access to my thoughts: potential access alone is insufficient to comprise a violation (Tavani & Moor 2001).

While interesting in themselves, these discussions have a limited bearing on the harm of privacy violation associated with surveillance. Whether privacy is a specific right or an amalgamation of several rights, or whether it is defined by access or control do not make a significant difference to the fact that a harm has been carried out. More pertinent perhaps is

the value of privacy. It may be that one interpretation of the value of privacy ranks it as being comparatively trivial next to other concerns, while an alternative interpretation may rank it as being almost as valuable as life. As it happens, there is not so great a disparity between interpretations as may be the case. Most authors acknowledge a range of values for privacy but tend to emphasize the particular aspect in which they are interested. For most it would seem as if privacy is indeed valuable for several reasons, but that its value does not compete with more basic human interests such as life, food and shelter.

Privacy is therefore valuable for a number of reasons, as seen in law, anthropology and philosophy. This raises a number of questions regarding the value of privacy which are worthy of clarification, namely whether it is possible for:

a) a person to voluntarily choose for his or her interests not to count in a particular consideration,
b) competing interests of sufficient gravity to outweigh this interest, or
c) a person to be wronged by the failure to give sufficient weight to his or her privacy interests.

In approaching the first of these, the game show Big Brother provides a helpful illustration. Contestants entered a house where they were cut off from the outside world and subjected to 24-hour surveillance by cameras and microphones within the house. The images from these cameras, and sounds from the microphones, were then made accessible to viewers on television and over the internet. This life without privacy was taken to new extremes in the 11th series of the show in the UK in which all the interior walls of the house were transparent and colourless, allowing for total visibility throughout. Contestants' genitalia were blurred before images were relayed onto the internet or television, but clearly the contestants were exposed to one another at all times.

Even in cultures which recognize a high degree of privacy, then, people may voluntarily choose for that interest not to count in a particular consideration, in this case how they should live for a limited period of time. This could also be true of exhibitionists who perform sexual acts in public or those who frequent nudist camps in which they wear less than would be commonly accepted in their society.

In addition to voluntarily choosing for one's privacy interests not to count in a particular consideration, there may also be occasions when those interests can be outweighed. Locke argues that while privacy typically increases one's sense of security there are also scenarios in which security benefits from a *lack* of privacy. Less privacy increases accountability within society with the result that there is a heightened disincentive to commit socially unacceptable acts; the constant gaze of others is a similar disincentive to politicking for personal advancement; and the lack of privacy can raise awareness of the mental and emotional states of others, providing for a more nurturing society (Locke 2010 pp. 71–3).

In these cases the subject's interest in privacy could be outweighed by the competing legitimate interests of society. I say legitimate as it is not acceptable for society to determine that it wishes to see *every* moment of the prime minister's personal life relayed as if he were living in the Big Brother house. There still has to be a just cause legitimating the surveillance as a *jus ad speculandum* consideration, along with further considerations of proportionality, necessity, etc.

Finally, if a person's privacy interests are not respected and that person has neither voluntarily chosen for those interests not to count, nor had them legitimately outweighed, then that person has been wronged by the failure to give sufficient weight to his or her privacy interests. This is true of the archetypal victim of the peeping Tom, wronged by the actions of his or her surveillant. It was also true of the deformed people such as Joseph Merrick (popularized as John Merrick in the film, *The Elephant Man* (Lynch 1980)) who were coerced into appearing in freak shows, and of those incarcerated in mental asylums in the Victorian era. In the latter case, inmates had an interest in being surveilled by the staff, and so their privacy interests might conceivably have been voluntarily chosen not to count or overridden on paternalistic grounds if they were deemed incapable of consent. However, there was no legitimate interest served in their being surveilled by the general public. The surveillance of these people by the public for little more than entertainment therefore wronged those subjected to the surveillance by failing to give sufficient weight to their privacy interests.

Hence there is evidence from international law, philosophy and anthropology for a universal interest in having and protecting privacy, although the amount of privacy may vary across cultures and eras. However, these privacy interests are neither inalienable nor

absolute. They may be voluntarily chosen not to count in particular considerations or outweighed by legitimate competing interests. A person whose privacy interests have not been given sufficient weight, though, has been wronged.

Privacy, while significant, is not the only relevant harm, though. There is a further possibility of harm arising from the specific information gathered by surveillance. The subject may become vulnerable as information, which he might prefer to keep secret and which could be used to damage him, is put into the hands of others. Once they possess this information, those others may use it to harm him. This harm may come from divulging the information to third parties (e.g. the revelation of an affair to a spouse) or from the surveillant acting upon it directly (e.g. discovering a phobia and then exploiting this). Even if this harm never arises there is a corresponding fear, should the subject become aware of the surveillance, that such a harm might occur and could impact the wellbeing of the surveilled subject irrespective of the further actions of the surveillant.

There is thirdly the possibility of control. Knowing that others hold information which might be used to harm him, the surveilled subject becomes vulnerable to a degree of control exercised by the surveillant or third parties to whom the surveillant has passed information gathered through surveillance. These parties may use the possession of potentially harmful information to coerce and control the subject, for example through blackmail. Once again, even if neither the harm of acting upon the information nor the harm of control are realised, the subject may still reasonably *fear* this control if he becomes aware of the surveillance.

Fourthly there is the concern that, while the last two harms would arise only from deliberate behaviour on the part of the surveillant, even with the best will in the world mistakes happen and information leaks out (Big Brother Watch 2011). The surveillant may inadvertently reveal the information he possesses over a drink with a journalist, or in a situation which he feels is in private but in which he is, ironically, himself being monitored. Likewise laptops, memory sticks and CDs containing sensitive information have been known to be stolen, or simply left on trains, park benches and other public places where they can be found and exploited by unscrupulous people.

Finally there is the possibility of discovering legitimate but embarrassing aspects of the subject's life. The information gained through surveillance might not concern criminal

activity but there may still be reasons for the subject wanting it hidden. In contrast to the aphorism that "if you have done nothing wrong you have nothing to hide" there are clearly situations in which a person has done nothing wrong but might nonetheless choose to hide the information regarding what they have done. For example, he might in private and consensual settings engage in activities of which society disapproves but does not deem to be illegal. A second example may be that she is planning a surprise party for her boyfriend which she would not want revealed to him. Or, thirdly, he may simply keep a diary, the publication of which would reveal to all just how mundane his life really was. He may not wish this impression of him to become public and so reasonably chooses to keep his diary private.

The likely individual harms of surveillance are hence privacy violations, vulnerability to harm and/or control (either deliberate or as a result of human error), and the possibility of legitimate but embarrassing information being uncovered.

3.4 Conclusion

This concludes the overview of the benefits and harms of surveillance. These are summarised in Table 2. Both benefits and harms have been shown to occur at the societal and individual level. While not providing empirical evidence of benefits or harms, this chapter has made appeal to the intuitive plausibility of the arguments presented. The chapter is intended as a reference tool and glossary for the remainder of the thesis.

Part II - *Jus ad Speculandum*

4. Just Cause for Surveillance

It is one of the oldest and best established principles of the just war tradition that wars should have a justified cause, as described by Augustine and Aquinas (Aquinas 2000 p. 1354), and agreed upon by almost all subsequent commentators. Similarly, the questions as to whether and when surveillance can be justified must include the issue of cause: what is the reason for the surveillance? As with the ethics of war, all the authors writing on surveillance ethics agree on this, and with good reason. Imagine two work colleagues, Andrea and Bob. One day Andrea starts logging in to Bob's computer to read his e-mail, she phones him every hour on the hour when he is at home, and she attaches a GPS monitoring device to his car to see where he is driving. If Andrea were doing this for no reason whatsoever then her activity would be bizarre and clearly wrong. If, on the other hand, Andrea and Bob work in security for an intelligence organisation and Andrea has good grounds to suspect Bob of selling state secrets to a foreign power then her behaviour stands a chance of being ethical.

This chapter will focus on justifying causes for surveillance. I have already argued that there can be harms associated with non-consenting surveillance (chapter 3). It follows that any surveillance should be justified in terms of warranting these harms.

Many of the considerations of justified surveillance rely on there being a just cause. The question of proportionality requires that a cause be identified in order that the harms can be judged proportionate (or not) to that cause. The issue of proportionality is covered in chapters 10 and 11, where I also look at the difference between the justifying cause and other benefits as factors to be weighed in considering proportionality. Likewise the necessity of surveillance can only be judged when the cause, and alternative measures for achieving the end associated with that cause, is known. Chance of success similarly requires there to be a cause in order to identify what would count as success, and correct intention correlates the intention of an agent with that agent's stated cause. In each of these conditions, then, it is important that there be a justified cause, and that that justified cause be recognised.

In thinking about justified causes for surveillance there is an important distinction to be made between surveillance which has the surveilled subject's consent and that which does

not. With the subject's consent, I as surveillant would be justified in my surveillance in more circumstances than I would without that consent. Hence contestants in the TV show Big Brother consent to surveillance for the chance to win a cash prize and some fame in the knowledge that the information returned by the surveillance will be witnessed by millions of people for their own entertainment (Channel 5 Broadcasting Ltd 2011). Were the contestants of Big Brother not consenting (as is the case for Truman Burbank in the film, *The Truman Show* (Weir 1998)) then this would, *ceteris paribus*, be unjustifiable. This is not to say that consent of the surveilled subject automatically justifies all surveillance of that subject. However, the considerations for consenting surveillance (such as concerns of exploitation and questions as to what counts as valid consent) differ from those for non-consenting surveillance. In keeping with the design of this thesis as discussed in chapter 1, this chapter will focus on non-consenting surveillance.

In this chapter I consider possible justified causes for surveillance of the non-consenting. In the first instance I briefly consider the surveillance of children and the severely disabled who are unable to freely offer consent, arguing that, in such cases, care of the individual provides a just cause for surveillance.

I then consider the notion of liability. Here I look at the case of self-defence to argue that there can be an uncontroversial justifying cause for non-consenting surveillance. This leads to the argument that liability forms a sufficient condition for a just cause. However, I argue, there are epistemic problems with liability, which raise the question whether people may be treated as liable when their actual liability is unknown. Under certain circumstances, which I explore in this section, I argue that they can justifiably be treated as liable.

Having looked at liability and being justifiably treated as liable, I consider whether the benefits arising from surveillance can provide a justified cause. I will avoid a straightforwardly consequentialist argument by denying that the benefits merely outweighing the costs provides a justified cause. However, I will argue that when the benefits *significantly* outweigh the costs, and those costs are minimized, then this may provide a justified cause for surveillance. Furthermore, only certain benefits should be considered as acceptable. The precise nature of these benefits will be discussed in chapter 10, but I will prefigure some of that discussion in this chapter.

Finally I look at the possibility of paternalism as a justifying cause. There are a number of different forms of paternalism which I examine across different contexts. My conclusion here is that in the case of competent adults paternalism does not provide a justified cause.

My conclusion is that there are justified causes which may contribute to an overall act of surveillance being justified. In the case of mentally competent adults these causes will only result from cases in which the subject of surveillance is liable to be targeted by surveillance (or can be reasonably treated as such) or where the benefits of that surveillance significantly outweigh the costs. That is, I will argue that liability and significant benefit are each sufficient conditions for providing a just cause for the surveillance of non-consenting mentally competent adults.

4.1 Surveillance of Children and the Non-Competent

There are groups of people who are unable to offer consent to surveillance but who benefit from that surveillance. These are children and those who are significantly mentally and sometimes physically disabled. By including the possibility of physical disability here I am allowing for extreme cases in which the disabled person is unable to communicate, such as through Locked-In Syndrome (Chisholm & Gillett 2005). In describing these groups as unable to offer consent, I am not including people who have simply not been asked for their consent, or those who live in regimes such that they are not reasonably able to express their opposition. Rather I mean those who are not competent to offer consent and also not competent to look after themselves unaided.

In such cases there is a duty of care to monitor these people. However, it would be wrong to suggest that they are *liable* for surveillance. They have done nothing to warrant being subject to surveillance. Furthermore, if someone failed to subject either a child or severely mentally/physically handicapped person to surveillance when it was in their best interests it would be neglectful and a dereliction of the duty of care. This is because both groups have diminished autonomy, and so require others acting on their behalf for their safety. I do not take this form of surveillance to be controversial but will return to more controversial cases of paternalism later in this chapter. There is therefore a justified cause present for surveillance of children and the severely mentally/physically handicapped person on the basis of a duty of care.

4.2 Liability

It is broadly accepted that one of the few justifications for killing another person is when it is necessary in self-defence. It seems reasonable then that self-defence can also provide a justified cause for surveillance if, through that surveillance, I can save my own life. If I am justified in *killing* someone who threatens my life then I am surely also justified in taking less harmful action to achieve the same end. The benefit will be the same (the sparing of my life) but the cost is considerably reduced (my assailant is subject to my surveillance *vice* being killed). Therefore, the surveillance of an assailant undertaken by me for the defence of my life appears to be justified. In other words, I have a justified cause for monitoring my assailant.

Assuming that the assailant in the above case is a mentally competent adult who does not consent to the surveillance, there is hence at lease one justified cause for the surveillance of a non-consenting mentally competent adult. In this case, the justification relates to the fact that the person to be subject to surveillance has made himself liable to surveillance as a result of his actions. Another way of stating this is to say that, to be liable for X is to do something which warrants the cost of X. To be liable for surveillance is hence to do something which in some way warrants the cost of surveillance.

4.2.1 Becoming Liable

Given that a person may be liable for surveillance it is important to ask *how* a person becomes liable for surveillance. To become liable requires an occasioning trigger: something must be done to effect the change in moral status from non-liable to liable. This is in contrast to an arbitrary switch which can happen at random. If, for example, I break a law then I render myself liable for punishment. If, on the other hand, I resign from my job then I cease to be liable for any responsibilities I once held as a result of being in that job. In order to move into or out of a position of liability a person must *do* something. I shall argue that this is always the case, and that liability cannot be imposed by another.

The need to perform an action to become liable is widely recognised in the just war tradition when consideration is given to people becoming liable to be targeted (e.g. they become combatants). It is a consistent theme in the tradition that to move from being a

non-combatant to being a combatant a person must do something to engage in the war, such as wear a uniform (Pfanner 2004; Corcione 1991 p. 4; US Supreme Court 1942), carry a weapon openly during wartime (De Vattel 2006 p. 513; 109th Congress 2006 sec. 948a; Corcione 1991 p. 4; Nagel 1972 p. 140), or otherwise openly engage in the conflict (Penafort 2006 pp. 144–45; Pizan 2006 p. 218; von Wolff 2006 pp. 473–74; J.T. Johnson 2000). Hence one's legitimacy as a target arises as a result of one's actions. Put another way, there is an assumption of an underlying right not to be targeted which is lost when an individual arms himself and dons the uniform of a state which is at war (Walzer 2006a pp. 144–45).

This could of course be challenged. It may be countered that it is possible for another person to effect this transition from non-liability to liability on a person's behalf, i.e. that a person can be *made* liable.

The concept of being made liable by another seems almost abhorrent. Nonetheless there are cases, such as military conscription in wartime, which suggest that it is at least plausible that a person becomes liable through the action of another. In the case of military conscription a person is coerced to don a uniform and carry a weapon in order to fight for his state. However, the conscript does retain free will: he can refuse and take the stance of an objector, although likely at some cost to himself. If he does not refuse, then by wearing a uniform and carrying a weapon he becomes liable to be targeted and killed by the enemy. The lack of obvious consent on the part of conscripts (or coerced consent if the cost of objecting is capital punishment) has meant that their moral status as combatants in war is a contentious issue, as discussed by Jeff McMahan and Michael Walzer (McMahan 2007; Walzer 2007; McMahan 2006; Walzer 2006b). However, I will argue that irrespective of his moral status, in the sense of whether or not he *deserves* to be targeted, the conscript is nonetheless *liable* to be targeted in war.

In the case of conscription there are at least three categories of person that are pertinent to considerations of liability. The first is that of the willing volunteer soldier. This person does not need to be conscripted, but it is plausible that he is conscripted on the same day that he becomes eligible to volunteer (such as his seventeenth birthday). Hence he is a willing conscript. The second category is that of the unwilling conscript. This person does need to be conscripted as he will not fight unless conscription forces him. Nonetheless,

having been conscripted he wears the uniform and goes off to war. The third category is that of the objector (conscientious or otherwise). This person is conscripted but refuses to fight, preferring to go to prison or even face execution rather than fight in (at least this particular) war.

In terms of liability, all three have done something. However, only the willing and the unwilling conscript have done something which makes them liable to be targeted as combatants in war. The objector may have done something which makes him legally liable to be punished by the state (e.g. refusing conscription), but in terms of war he is a non-combatant and should not be targeted by enemy soldiers. This may seem harsh on the unwilling conscript. He has, after all, been coerced into becoming a soldier. Despite the coercion, though, he has performed an action (dressing and acting as a combatant) which the objector has not. What makes him liable is not his having made the choice to become a combatant, but rather his acting as a combatant and thereby losing the right not to be targeted. He has donned a uniform, taken up arms in wartime and openly engaged in war, thereby distinguishing himself from non-combatants who do none of these things. Furthermore, the existence of the objector suggests that the unwilling conscript did have a choice, however unpalatable, not to become a combatant. As such the unwilling conscript has not been made liable through conscription, but rather through his own actions.

I referred above to a distinction between liability and desert, a distinction which is worth emphasising at this point. By wearing a uniform in times of war the conscript has not necessarily done anything wrong such that he would deserve to be targeted. Even if he had done something wrong, such as fighting for an unjust side in a war, it would not *necessarily* follow that he deserved to be targeted. As McMahan succinctly states, "To say that a person is liable to be attacked is not to say that there is a reason to attack him no matter what; it is only to say that he would not be *wronged* by being attacked, given certain conditions, though perhaps only in a particular way or by a particular agent [emphasis in original]" (McMahan 2005 p. 7).

I am now in a position to ask what a person must do to entail their moving from a state of non-liability for surveillance to a state of liability. The most obvious answer to this is that it is the performing of some action which makes me liable. For example, if I walk into an airport with a bomb visibly strapped to my chest then this would indeed warrant my

receiving special attention. Likewise, if I murder or rape someone then I become liable for surveillance. It is not merely committing crimes, or even moral wrongdoings, that render a person liable for surveillance, though. In war it seems not only prudent but right to monitor the positions and movements of the enemy. Yet the enemy may not have committed a crime or wrongdoing. Hence liability in the case of surveillance need not depend on a crime or moral wrongdoing. Rather, it depends on a person or people performing an action which warrants the cost of surveillance.

4.2.2 Which Actions Warrant Surveillance?

It is sometimes claimed that war is a warranted response only in self-defence when one state attacks another (United Nations 1945, Article 51). This has become more controversial in recent years when, following the civil war in Rwanda there were broadly felt to be grounds for international military intervention to prevent bloodshed (United Nations 2013; Best et al. 2008 pp. 42–24; Kuperman 2001; Ludlow 1999). Even taking international intervention into account, though, this would still leave only two commonly-accepted justifications for engaging in war.

While it would be convenient to identify a similarly limited number of actions which render a person or people liable for surveillance, this is not possible. At the heart of determining which actions make a person liable to be subject to surveillance lies a consideration of proportionality: the cost of surveillance weighed against the cost of particular crimes. This problem of proportionality is compounded by the fact that there is not just one form of surveillance. Surveillance ranges from keeping an eye on people who may look a little suspicious to a state monitoring the phone calls of its citizens.

Given that there are a variety of actions and a variety of forms of surveillance, the abstract definition of liability can go no further than saying that such liability arises from some actions. To go further would require a case-by-case examination. This may appear weak, but a number of points should be borne in mind. Firstly, liability arises from some actions. It is fairly easy to imagine such actions, for example murder, rape, and kidnap. Secondly, I am not claiming that liability arises from all actions. There are clearly actions which may not cause one to be liable for surveillance, such as those that most people perform every day (i.e. eating breakfast, getting dressed, etc.). Thirdly, this is not intended to be the end

of the discussion. This section has recognized liability as sufficient to provide a justified cause to subject a person or people to surveillance. The details as to precisely which actions render a person liable will need to be decided on a case-by-case basis. That falls outside the scope of this thesis.

4.2.3 Purpose

A final point of clarity is needed in establishing the purpose of the surveillance. I have argued that a justified cause of surveillance is found in a person being liable for that surveillance. Yet as it stands this is not sufficient to justify surveillance. In order to be justified, and to provide the grounding for other principles such as proportionality, necessity and chance of success, there must be a justified end to that surveillance. Throughout the forgoing discussion I have associated the justified cause with liability, and that liability with certain actions. This being the case, it is reasonable to suggest that the justified end of the surveillance would be to apprehend the agent who has performed the action and/or to prevent the action from occurring.

This may be too demanding, though. It is unlikely that surveillance alone could achieve either apprehension or prevention. Rather it is likely to be a part of a process aimed at achieving either or both of these. Surveillance therefore has a justified cause *if* an entity (a person or group of people) is liable *and* the surveillance will be used towards preventing the action that makes that entity liable from occurring or apprehending the entity which has performed the action.

Having the goal of being used to apprehend an agent engaged in an act which warrants the harms of surveillance and/or prevent such an action helps to ensure that the surveillance is not gratuitous, and that it is not complicit in ignoring an action which should be addressed. As noted above, it also provides grounding for other principles in *jus ad speculandum*. Hence in asking whether an act of surveillance is necessary, that necessity pertains to the goal of apprehension and/or prevention. The same is true as regards the principles of chance of success, in determining what success consists of, and proportionality.

4.2.4 The Appearance of Liability

In discussing the liability of conscripts above, I argued that the unwilling conscript was liable to be targeted owing to his actions. What, though, if his actions posed no actual threat to the enemy? What if he decided to always fire above the heads of enemy soldiers so as to not actually kill anyone, and was able always to act on this decision. Might he not, in this case, merely *appear* liable but not actually *be* liable?

I have argued that liability does not depend on the moral status of a person. In this case, the peaceable unwilling conscript may be less blameworthy than one who shoots to kill (although he may not, if he is fighting in defence of a just cause then by not shooting to kill he may be promoting the chances of an unjust cause succeeding in the war). Independent of his moral status, though, is the fact that he has acted in a way that makes it reasonable for the enemy to believe that he is a threat and is as such liable.

The same approach carries over into surveillance. Imagine a man walks into a bank with a paper bag over his head, brandishing a toy gun. It may be that he is painfully shy and has just bought the toy for his son. Nonetheless, by acting in this way he has made himself liable to be subject to surveillance.

It is worth restating then that there is an important distinction between desert and liability. A person does not need to deserve to be subject to surveillance in order to be liable to be subject to surveillance. In response to the above question then, neither the peaceable unwilling conscript nor the man with a bag on his head has the mere appearance of liability. Rather both are liable, either to be shot at or subjected to surveillance.

The reason for this is based on an epistemic problem that the person in a position to react to the conscript or the man with the bag does not know their intentions. A comparison can be drawn here with pre-emptive wars. As noted above, war is typically justified as a response to an attack on a state's sovereignty. However, there are times in which the war may pre-empt that aggression. That is to say, war is justified even though no act of aggression has (yet) been carried out. In these cases it is the manner in which the target state is acting that renders it liable.

Within the just war tradition, pre-emptive wars are often accepted if it is clear that a person is about to be attacked. Thus, provided that other just war conditions are met, imminence is typically taken to be sufficient to justify a pre-emptive attack in war (Struhl 2005; Ignatieff 2004). This has led to the distinction, at least in recent discussion, between pre-emptive wars and preventive wars, the difference being a matter of time. Pre-emptive wars are defined as responses to imminent threats of attack and are typically seen as just. Preventive wars respond to less imminent threats and are often seen as unjust (J.T. Johnson 2007). The justification for the difference seems to be that the more imminent the attack, the more likely it is that war will ensue. By contrast, the less imminent the attack, the greater the chances are that the enemy posing a threat will change its mind. Yet the timescale involved in imminence is uncertain at best. How soon is "imminent"? Is it one day, one week, one month, or one year? There seems to be no objective measure as to what is imminent.

Whitley Kaufman has criticised this notion of imminence as failing to reach the heart of the matter (Kaufman 2005). Employing a *reductio* argument, he asks why, if one has to wait for war to be imminent because the enemy might change its mind, a state is justified in fighting when that enemy crosses its border. Surely there is still the chance that even then the enemy might change his mind and retreat. Rather, Kaufman argues, we should be looking not to the timescale of the attack but the evidence for that attack. After all, the German army sat on the border of France for months during the "Phoney War" of 1939-40 in such a way that war ceased to be seen as imminent, but a host of evidence pointed to its inevitability.

Kaufman's claim here is illustrative of my comments on liability. It is evidence and not timescale which is of central importance in justifying pre-emptive/preventive wars. It may be that evidence and timescale are often conflated, as it is often only when war becomes imminent in time that the intentions of one's enemy become apparent, but this is not necessarily the case as demonstrated by the Phoney War. In this case war was not imminent in time but it was inevitable nonetheless. Sufficiently strong evidence to establish a clear intention to attack within a reasonable timeframe (i.e. not 20 years in the future in which time not only minds but leaders are likely to change) is therefore enough to justify a preventive attack.

In the same way, with surveillance the imminence of an action alone is insufficient to provide a justified cause. Evidence is both necessary and sufficient to establish the liability of a person to be subjected to surveillance. Whether that person deserves to be subjected in this way is a separate question. The unwilling conscript and the man with a bag on his head in the bank are both, therefore, liable.

4.2.5 Treated as Liable

The issue of evidence raises a further concern. What of cases in which a person has done nothing to make themselves liable but there is evidence of them being liable? Take for example the case of Georgina, who has done nothing which would render her liable for surveillance. However, a spiteful neighbour contacts the police to suggest that Georgina has done something which does warrant the cost of surveillance. If I am correct that liability cannot be imposed by another (and hence Georgina is not liable to be subject to surveillance) then how is the potential surveillant to respond to such a situation?

One response would be to accept that the surveillant is subject to moral luck. While there may be a fact of the matter whether or not a person is liable, the potential surveillant may not have this knowledge. Indeed, knowledge of liability might only come as a result of the surveillance. Hence the surveillance can only be justified *post hoc*, when the actual liability of the person subject to that surveillance is known (if then). This is a difficult position for the surveillant to find herself in: she cannot predict the outcome of the surveillance but if it falls one way she will be justified, if it falls the other then she will not. If she carries out surveillance on Georgina, who has done nothing to warrant that surveillance, that surveillance will not be justified.

A second response seeks to avoid the difficulties of moral luck. Here the surveillant can seek to justify her surveillance on the basis of evidence (Nagel 2012 pp. 24–38). If there is reasonable evidence that Georgina has done something that would warrant the cost of surveillance then she could be treated *as if* she were liable. Hence when liability is unknown, reasonable evidence of liability can justify treating the person as liable. This is of course similar to what I have said about liability and pre-emptive war insofar as both look to evidence to establish how the surveillant should respond. The difference is that in the case of the pre-emptive war one side has acted to make itself liable by providing

evidence of a threat. In the case of Georgina she has not acted in any way that would make her liable. Nonetheless, there is evidence that she is liable. How should a surveillant proceed in this situation? Can he treat her as liable even if she is not?

Before answering that, there is a further case in which a person is liable but there is no evidence of their liability. This may be seen in numerous instances of unsolved crimes in which it is clear that an action rendering someone liable for punishment has occurred and yet there is no evidence to indict anyone. To give a name to this case, imagine that Helen has murdered her partner in such a way that the police do not even suspect that she is the murderer. Helen has committed what some would call "the perfect murder".

There are therefore four possible options regarding liability and evidence. These may be categorised in the following way:

1. Liable with evidence of liability
2. Liable with no evidence of liability
3. Not liable with evidence of liability
4. Not liable with no evidence of liability

Of these four options, (1) clearly provides a justified cause for subjecting a person to surveillance while (4) states a situation in which there will be no justified cause based on liability for subjecting a person to surveillance. (3) depicts the situation of Georgina while (2) that of Helen, the "perfect murderer" who gets away with it.

The challenge, when these options are coupled with the importance of evidence, is that from the perspective of the surveillant (1) and (3) look the same, while (2) and (4) also look the same. The objection to basing surveillance on evidence is thus that a liable person (2) may not be subject to surveillance despite their having acted in such a way as to warrant it, and that a non-liable person (3) may be subject to surveillance despite their having done nothing to warrant it. Georgina, while not being liable, is therefore subject to surveillance while Helen, being liable, is not subject to surveillance. This seems to be wrong.

While the cases of Georgina and Helen are unquestionably challenging, they are not without precedent. If one looks to punishment through judicial process, a similar situation emerges. Criminals may be guilty and yet get away with their crimes while the innocent,

owing to evidence against them, may be imprisoned. This situation is broadly accepted, though, as the judge and jury cannot know the fact of the matter as to whether a person is guilty. They merely have the evidence as presented to use as a basis to establish guilt. There is hence an analogy between punishment and surveillance in that both are of necessity reliant on evidence rather than the objective fact of the matter.

An objection to this analogy may be raised that in court the evidence must establish "beyond reasonable doubt" that a person is guilty. If that were to be extended into surveillance such that there must be evidence establishing that a person is liable "beyond reasonable doubt" then most surveillance that is commonly accepted would need to be rejected. This, though, draws the analogy with only one type of judicial proceeding. If one looks rather to civil cases then the evidence must merely weigh in favour of a person being guilty in order for them to be found such. I contend that this is the correct analogy to be drawn in the case of surveillance. Hence the evidence of liability does not need to be conclusive in order for the surveillant to have justification for treating the subject as liable. Rather the weight of the evidence must be in favour of her being liable in order to treat her as such.

Thus it is the evidence of liability that justifies surveillance rather than liability itself. That is, the justification for the surveillance must come from the perspective of the surveillant, and the evidence available to him, rather than from an objective truth to which the surveillant is not privy. Despite her *not* being liable, then, the evidence against Georgina provides a justified cause to subject her to surveillance. Furthermore, despite her *being* liable, the lack of evidence against Helen means that there would be no justified cause to subject her to surveillance.

4.3 Benefits of Surveillance

I have argued so far that it is not the case that everyone is liable for surveillance. Instead one can become liable for surveillance as a result of one's actions, or may be treated as liable if there is good evidence of one's intentions and actions involving one in certain actions. It is not the case that any action justifies liability, but rather particular actions which warrant the harms of surveillance. Given that there is often a lack of knowledge regarding a person's liability, I have argued that a person may justifiably be treated as liable

provided that there is good evidence of the actions which would render them liable. It is important also that the gravity of the wrongdoing be weighed against the potential harms which surveillance may occasion. Finally the end of the surveillance must be to prevent the action and/or apprehend the agents to which the surveillance pertains.

However, liability is not the only ground for providing a justified cause for surveillance. Imagine a sociological or psychological survey of people's behaviour in a public place, such as those carried out on traffic flows or the behaviour of people on the London Underground. Here consent has not been sought from the participants. Indeed, were it sought then knowledge of the surveillance could affect the outcome of the survey. The surveillance is hence of the non-consenting person. At the same time, none of the participants is liable, nor is there evidence for treating any of them as liable. Nonetheless the surveillance may be justified.

The benefit to come from the surveillance in these cases (improvement of traffic flow and the recognition of potential suicides respectively) is significant, whereas the harm is, at least on first impressions, limited. There may be harms arising from the abuse of the surveillance, but the surveillance itself does not obviously lead to the harms discussed in chapter 3 such as chilling effects, behavioural uniformity, or invasions of privacy.

In these cases the surveillance is justified because the benefits are *significantly* greater than the harms associated with it. To say that such surveillance is justified for this reason is not an appeal to consequentialist theory owing to the importance of the significant benefit over the harms. It is not a mere cost-benefit analysis in which the outcome is justified if the benefits barely outweigh the costs. Rather there has to be an obvious and recognisable benefit *and* minimal costs to those subject to the surveillance. Furthermore, not just any benefit would provide this justification. Certain benefits, such as the voyeuristic satisfaction of a surveillant, should not count. In a straightforward consequentialist consideration, should the surveillant receive vast amounts of voyeuristic pleasure from the surveillance, and those subject to the surveillance experience little harm, then the surveillance would be justified. By contrast, I argue that benefits such as these should not be weighed in the balance. This will be discussed in greater depth in chapter 10 when looking at proportionality.

Hence in the aforementioned studies of traffic flow and people's behaviour on the Underground, significant benefits can be gained from understanding how drivers behave on certain road systems to improve efficiency and how suicidal people act on the Underground to enable active intervention. At the same time, minimal harm is visited on those subjects of these studies, even though they do not consent to being monitored.[4]

This argument from significant benefits contrasts with the argument from liability. In the argument of justified cause based on liability, once a person has been found liable, or is justifiably treated as liable, then the *jus in speculando* consideration of proportionality might allow for a high level of intrusion into that person's privacy (see chapters 11 and 12). By contrast, the argument that significant benefits coupled with minimal harms provide a justified cause for surveillance limits the harms that can be visited on the subject(s). I will argue in chapter 11 that the harm of a particular form of surveillance must be in proportion to the justifying causes. Hence a cause based on this justification will not allow for similar levels of intrusion into personal privacy or other harms as would a cause based on the justification of liability.

The requirement for harms to be minimal thus introduces an important distinction between justified causes based on liability and those based on significant benefits. In the former case the harms visited on the liable person can be significant. If the action and evidence warranting the surveillance justifies it, the surveillance can be very intrusive. Justified causes based on significant benefits, though, cannot justify the same level of intrusiveness or harm more generally.

One objection that could be raised here is why not just appeal to a straightforward consequentialist theory or at least to the consequences of surveillance in order to determine what is a justified cause? In response to the first of these I raised and dealt with this objection in chapter 1 as failing to respect individuals. There I used that argument to justify not employing consequentialist theory to surveillance in general. Here I appeal to the same reason for not using it to provide a justified cause. Furthermore, and related to the second part of the objection, a simple appeal to consequences would mean that a minor benefit could justify potentially very harmful surveillance. If, for instance, benefits and harms

[4] This is a stipulation. It may be that the methodology of certain studies, or unintended uses of their results, could in practice harm the participants.

were equal, then the fact that 51 out of 100 people benefited from surveillance of the minority then this would be sufficient to justify the surveillance of the other 49. This would be tantamount to a tyranny of the majority.

To illustrate this tyranny of the majority, imagine that a state was comprised of 51% white people and 49% black people. The white people do not trust the black people not to graffiti public property and so subject them to 24/7 surveillance to ensure that the black people do not deface public property. To avoid this I am arguing that the benefits need to be significant (i.e. a small net benefit such as discussed here would not suffice) and the harms minimal (i.e. 24/7 surveillance, with the harms that that would entail, would not typically class as minimal). Efforts should therefore be made to reduce the harms as much as possible to limit the potential side effects of surveillance whose cause is justified in this way. The significance of the benefits coupled with the minimized harms prevent situations arising in which a tyranny of the majority may take effect or where very minor benefits would provide a just cause. At the same time, this opportunity for surveillance based on significant benefits and minimal harms allows for certain types of surveillance to take place which could not be justified by an appeal to liability. As noted already, I shall return to the discussion of which benefits should count in chapter 10.

There is a further objection which may be levelled at this attempt to justify surveillance on the grounds of the benefits it provides. This objection holds that once this justification has been accepted then it can be used to justify more controversial surveillance, typically by the state of its citizens. Hence broad-scale CCTV systems in response to acts of terrorism may be endorsed as they "provide significant benefits to society." In response to this objection it is important to remember that the benefits need to be significant *and* the harms minimal. If this is not the case then the surveillance is not justified.

4.3.1 Deterrence

There are cases in which surveillance seems to be justified by appeal to deterrence. This has been discussed as an aspect of liability in which the liable person may be prevented from carrying out an action which warrants surveillance. However, it may be that deterrence is justified in situations where there is no liable person. Indeed, it may be as a direct result of the existence of deterrence that there are no liable people.

Imagine an airport in which there were no terrorists or other trouble makers. In fact, no-one using this airport does anything that would render them liable for surveillance. As such, liability cannot be the justification for surveillance of the airport. Nonetheless, surveillance would seem to be valuable. In its absence, let us stipulate that terrorists would see the airport as a "soft target" and plant a bomb there. Assume that if there were surveillance then the terrorists would not plant a bomb there. Under these circumstances the surveillance would be justified even though no-one has acted to make themselves liable, nor is there any evidence to treat anyone as liable.

The reason for this justification is to be found in the benefits of the surveillance (deterring the terrorists from planting a bomb) compared with the harms visited on the non-liable users of the airport. These harms should, as noted, be minimal. That is, if the surveillance invaded people's privacy, or caused chilling effects or other harms raised in chapter 3, it would be harder to justify on these grounds. If such harms were visited on non-liable users of the airport then the justified cause would need to be grounded rather in an appeal to liability. Such an appeal may be made to the liability of persons, if there were evidence suggesting that individuals were targeting the airport, or the liability of place, if there were evidence suggesting that the place was a target. The liability of places will be discussed in greater depth in chapter 12.

4.4 Paternalism

I have argued that in order for there to be just cause for surveillance, a person must either be liable for that surveillance, or that they be justifiably treated as liable as a result of reasonable evidence of some action which would render them liable, or that there are significant benefits and minimal harms resulting from the surveillance. Earlier in this chapter I also claimed that there are some cases of justified surveillance in which the party subject to surveillance has clearly done nothing wrong and so is not liable for that surveillance. Nonetheless the surveillance is justified because it is in the surveilled subject's best interests. The cases I suggested were of children and the severely mentally handicapped, that is those who are not fully competent.

While the surveillance of children and the severely mentally/physically handicapped is uncontroversial, it is important to ask whether there might ever be just cause to carry out

surveillance of an autonomous person who was not liable or justifiably treatable as such, and who did not consent to that surveillance? That is, can paternalism provide another just cause for surveillance in cases where there is no liability? Unlike the above scenario, forcing surveillance upon an autonomous person would be controversial. As Onora O'Neill has argued, interfering with an autonomous person's will without their consent (i.e. paternalism)[5], through subjecting them to surveillance that is neither wanted nor warranted, fails to treat them with respect as persons, as ends in themselves and should not be undertaken lightly (O'Neill 1985; O'Neill 1984).

This is not a wholly theoretical exercise. Dictatorships such as the GDR carried out extreme levels of surveillance on members of the public, both when they were in public but also in their own homes. Attempts were made to justify this, stating that it was in the interests of the people. Both at the time and subsequently it was reasonable to suspect that a significant minority (if not a majority) did not desire this surveillance (see, for example, Funder 2004). Nor is this limited to totalitarian states. Liberal democracies such as the UK have seen a rise in the number of CCTV cameras monitoring public spaces. In this case, the surveillance is limited to public space and does not encroach into people's homes. Again, the use of CCTV has been justified by Andrew Rennison, the UK's CCTV Commissioner, as being "in the best interests of the public" without there being clear evidence that it is what the public wants (Reeve 2012). Indeed, there is some evidence (through the existence of anti-surveillance lobby groups such as *Big Brother Watch* and *No CCTV*) that at least a significant minority does not desire this surveillance. Similar paternalism can be found in CCTV signs which proclaim that recording is taking place "for your safety" (Kuklowsky 2011; Barr 2008). There is also scope for communities to carry out paternalistically-justified surveillance on their members for religious or ideological reasons (Raine 2009) and/or individuals on one another if, for example, a wife is concerned her husband is a secret alcoholic and resorts to monitoring his behaviour to discover where he is hiding alcohol in the home.

It could be objected that the defence of surveillance being "in the best interests of the public" or "for your safety" could be political rhetoric or to quiet dissent, rather than an

[5] Although the interference with someone's will with their consent may seem incongruous, there are cases in which this occurs. One example would be a person choosing to visit a hypnotherapist in order to have his or her desire to smoke removed through hypnosis.

attempted justification. If this is so then the actual claims are disingenuous and should be rejected in favour of the underlying justification. Whether the claims are sincere or not, though, the fact remains that they are given and should therefore be dealt with and responded to.

In looking at paternalism as a potential just cause for surveillance, I will consider first the argument from the perspective of the state as authority. I take the case of the state (as illustrated above) to be the most common. However, there are concerns which may be specific to state surveillance justified by paternalism which are not relevant to surveillance carried out in a community or by individuals. Hence I will start with a general consideration of types of surveillance. From there I shall apply these types to the state, then to a community and to individual scenarios to determine whether paternalism can ever provide a justified cause for the non-consenting surveillance of fully autonomous people. Finally, I will respond to some hard cases to demonstrate that my position is consistent and intuitively plausible. My conclusion will be that, with the possible exception in which the will of an individual contravenes the will of a group to the detriment of that group, genuine acts of paternalism which over-ride the voluntary decisions of autonomous, mentally competent adults cannot be justified. As such, paternalism cannot form a justified cause for surveillance.

4.4.1 Types of Paternalism

I have described paternalism as the interference with an autonomous person's will, without their consent but for their own benefit. There are differing lengths to how far one might consider going in this interference, though. Hence there are several different types of paternalism.

The first type of paternalism involves interfering with a person's will to the extent that the interferer is able to establish whether the person interfered with is autonomous and acting voluntarily. If the person is found to be autonomous, then the interferer ceases her interference at that point. If not, then the interferer is able to act in the best interests of the non-autonomous person. This Joel Feinberg describes as "soft paternalism" (Feinberg 1986 pp. 12–16). To illustrate, imagine a man about to jump off a bridge in an act of suicide. According to soft paternalism it is acceptable (it may even be deemed a duty) to

interfere with him in order to make an assessment of his voluntary action and mental competence. If he is acting voluntarily and he is mentally competent then no more interference is permitted. If he does not meet these criteria then further interference is justified.

A second type of paternalism involves persuading a person to change their mind based on what the interferer perceives to be in that person's best interests. Obviously the term "persuasion" can have a number of euphemistic undertones. I take it here at face value to mean rational persuasion through argument based on reliable evidence. Julian Savulescu refers to this as "rational non-interventional paternalism": rational through the use of argument and non-interventional because it stops short of forcing the person to adhere to the interferer's will (Savulescu 1995). One example which Savulescu provides is a doctor advising a patient what the doctor believes is in that patient's best interests, all things considered. Returning to the suicidal man on the bridge, the rational non-interventional paternalist would condone the use of rational argument to persuade the man not to kill himself.

A third type of paternalism goes further than rational persuasion to introduce hard incentives and disincentives. On a state level, taxes on alcohol and cigarettes are a means of giving people incentives to do what the state believes is in their best interests. This is less coercive than imprisonment as it allows the agent greater freedom to choose to smoke and drink than would be the case if there were the penalty of a custodial sentence. It is, though, more forceful than mere argument. For the suicidal man this would involve offering him care and support to overcome his problems if he does not enact his suicide, or perhaps threatening to impose a cost on someone he values if he does go through with it. I shall call this incentive paternalism.

I have said that incentive paternalism may involve positive incentives or negative disincentives. It is beyond the scope of this chapter to clarify the difference between an incentive and a bribe, although clearly a positive incentive may be seen to be (or may actually be) a bribe in some contexts. For the purposes of this chapter I will assume that:

> the purpose of an incentive is also to give someone a reason to act in a way they would not do otherwise, such as work harder, or take risks. In this respect it is similar to a bribe. The difference is that the cost involved - the extra work or the risk

> (for example, when divers are paid 'danger money') - is borne by the person accepting the incentive. Where there is a cost or negative impact that will be borne by someone other than the person accepting the incentive, the reward is open to being construed as a bribe. It would definitely constitute a bribe in cases where agreeing to negative impacts that will affect others amounts to unethical behaviour. Similarly, if the action encouraged by the reward is unethical, illegal or unprincipled in other ways, accepting/offering the reward is a case of bribery rather than incentive (Rawles 2002 p. 14).

A fourth type is what has been called, somewhat paradoxically, "libertarian paternalism", which has been endorsed by politicians such as Barak Obama and David Cameron (Lawrence 2010; McSmith 2010; Thaler & Sunstein 2009). This involves prompting, or "nudging", a person to perform a certain action through the use of subtle suggestion and incentive. Richard Thaler and Cass Sunstein's book, *Nudge: Improving Decisions about Health, Welfare and Happiness* opens with an interesting case study. A friend with an interest in nutrition who works in a local school canteen notices that children in the canteen tend to buy food which is placed at eye level. Realising this the friend is faced with a dilemma: which foods to put at eye level? She can put the healthiest foods there, which would be in the children's best interest but could be taken to be paternalistic; she can arrange the food at random, which would mean that if this approach were employed across several schools some pupils would have a healthier diet than others based purely on which school they attended; she could try to arrange the food such that the children will buy what they would have bought anyway, but she doesn't know what they would have bought as they tend to buy what is at eye-level; or she could arrange the food such that she maximises profits for the canteen.

Thaler and Sunstein's conclusion is that the friend should clearly try to maximise the health benefits of the children and so place the healthy food at eye level. The friend cannot help but affect the choices made by the children and so she ought to influence those choices for the better (Thaler & Sunstein 2009 pp. 1–6). Given that I have stated that I do not see a problem (broadly speaking) with acting paternalistically towards children, imagine that the scenario takes place in a work canteen, rather than a school. Hence the targeted individuals are autonomous, mentally competent adults, rather than children.

There is some debate as to whether such an approach is consistent with liberal democratic principles. At one level, as Thaler and Sunstein suggest, these nudges occur anyway. The

workers in my adapted example will tend to buy what is at eye level. Recognizing this, it seems foolish not to ensure that the healthiest option is presented at eye level. At the same time this feels manipulative and undermining of debate. Perhaps the workers, on discovery of this trend, should be allowed a vote on what is placed at eye level in the canteen?

This, though, would be to make assumptions about the implementation of such nudges. It is not necessary that the nudge occurs without debate. It is quite feasible that the canteen explains to the workers why they have rearranged the food displays. It might even be that the canteen seeks the workers' approval for any such changes. In the latter case, though, seeking approval or some level of consensus is not paternalistic, at least as I have defined it above. If this is the course chosen then it is not a form of paternalism. Hence the options for the libertarian paternalist, to be truly paternalistic, are either to adopt the nudge without discussion, or to do so with some explanation but without seeking feedback. In order to be paternalistic, in the sense in which I am using the term, the act must be non-consenting and intended to benefit those who haven't consented.

The fifth and most extreme type of paternalism involves actively overriding a person's autonomous decision to act in their best interest. This Feinberg calls "hard paternalism" (Feinberg 1986 p. 12). Such hard paternalism in the case of the suicidal man would condone physically wrestling him away from the edge of the bridge to safety, as well as additional actions taken to prevent further possible acts of self-harm (i.e. getting him checked into a hospital where he can be monitored and kept away from sharp instruments).

4.4.2 Application

In what follows I shall apply each of the different forms of paternalism to the respective groups (state, community and individual). Having done this I will then respond to each of these applications.

4.4.2.1 State

To apply each of the five types of paternalism to surveillance, imagine a case in which a government wishes to install CCTV cameras in public spaces against the wishes of its citizens. I shall assume here that the government is motivated by a genuine desire to protect the citizens and believes that the cameras will help to do this.

I shall also assume that opposition to the government, at least on this policy, is 100%. This is to simplify the situation and maintain a level of clarity in dealing with paternalistic decision making. Once the numbers in opposition to the government fall below 100%, and particularly once they fall below 50%, then the question becomes as much an issue of the tyranny of the majority as it does paternalism. In the former case the question is to what extent the individual should be protected from the harms imposed by surveillance. Hence it is generally taken that slavery should not be permitted, even if 99% of society wishes it to be legalised. On the other hand, if 99% of society wishes for shops to be allowed to trade on Sundays and 1% objects then it is generally taken that the wishes of the 1% should be overridden. I shall return to this question below, but for now will assume unanimous opposition by those not in government.

The soft paternalist position will involve questioning the autonomy of those citizens and the voluntary nature of the objections. If the citizens are found to be autonomous and voluntary in making their objections, then the cameras should not be installed. The rational non-interventional paternalist position will try to go further and argue with the citizens that they are wrong, that the cameras are there for their benefit, and that they *should* want them installed. However, if the rational non-interventional paternalist fails in her argument she will, like the soft paternalist, respect the citizens' wishes.

The incentive paternalist will go further than the soft paternalist or the rational non-interventional paternalist and offer additional benefits such as tax breaks to people who agree to have cameras facing their property, or possibly fines for those who refuse. Hence citizens can refuse to comply but it will cost them to do so. The libertarian paternalist will go further still in introducing mechanisms into society to influence behaviour in such a way that the existence of the cameras is at least tolerated, if not welcomed. In this case the citizens can object, but owing to the mechanisms introduced they are less likely to do so. Perhaps all new traffic lights which are erected will be fitted with CCTV cameras unless residents register that they do not want the cameras. Finally, the hard paternalist will override the citizens' objections and install the cameras anyway, firm in the belief that they are in the citizens' best interests.

4.4.2.2 Community

Broadly speaking, using the same example of installing CCTV in the case of the community as I have just done in the case of the state, the application will lead to similar outcomes. The significant differences between the community and the state in this situation are that firstly the community typically has no morally legitimate coercive power over its members in the way that the state has. This means that the power of the individual to resist the community is greater than the power of the individual to resist the state, because ultimately the community can do less than the state to overcome this resistance. Secondly the community is likely to have weaker boundaries than the state. By this I mean that it is likely easier to enter or leave a community than it is a state. In transferring between communities one does not require passports, visas and possibly also the learning of a new language. Hume's critique of Locke's social contractualism[6] therefore has less force over a community founded on contract than a state founded on contract (Hume 2008 p. 283).

A third difference is that there are communities which are, potentially at least, not based on contract. This may be true of some religious or ideological communities. Typically these are entered into freely. If not then the members have either been kidnapped and subjected to the community, which is clearly wrong, or were born and raised in the community. Likewise all members should be allowed to leave the community freely. To disallow this would amount to false imprisonment, although in practice it may be very difficult for a member to leave the community owing to peer pressure or fears of being able to cope without the support of the community. In entering and choosing to remain in the community, though, members may waive their right to autonomy in some areas over which the leadership of the community exercises authority (e.g. the choice of whom to marry or how to raise children). If this is the case then the members have essentially consented to the leadership of the community acting in their best interests, irrespective of their wishes in

[6] Hume argued that Locke's notion of the social contract in which citizens were free to leave a state with which they disagreed (and hence implying that those who did not leave gave tacit agreement to the construction of the state) was flawed in practice. "Can we seriously say, that a poor peasant or artisan has a free choice to leave his country, when he knows no foreign language or manners, and lives, from day to day, by the small wages which he acquires? We may as well assert that a man, by remaining in a vessel, freely consents to the dominion of the master; though he was carried on board while asleep, and must leap into the ocean and perish, the moment he leaves her" (Hume 2008 p. 283).

particular cases. While an act may therefore go against the wishes of a member of that community, the fact that that member, *qua* member, has consented to a system of authority within the community means that such acts are, broadly speaking, unproblematic. Ultimately the member may leave the community although, as I have already said, this may be easier said than done for practical reasons. If this is not the case then there is a graver problem of false imprisonment.

Bearing these differences in mind, we can imagine a community, such as a neighbourhood watch scheme which exists to provide mutual support to members by watching a neighbour's property for them when those neighbours are on holiday, deciding to install CCTV cameras for the protection of property (i.e. to identify and deter burglars). This could involve paying for and installing one camera on every house in the community. However, imagine that one person in the community is resistant to this decision. The options of the community are therefore to:

1. ensure that the objector is acting voluntarily and autonomously in his resistance (and if so not to impose the cameras on him) – soft paternalism;
2. try to persuade the objector that the presence of the cameras is to his advantage (but if this fails not to impose the cameras on him) – rational non-interventional paternalism;
3. offer the objector an incentive to accept the cameras through offering to pay for his share or threatening to eject him from the community's neighbourhood watch programme – incentive paternalism;
4. introduce mechanisms into the community which will encourage the objector to accept the cameras. This might involve talking about them as a status symbol if the objector is known to be one who likes to "keep up with the Jones'" or applying a similar form of peer pressure – libertarian paternalism; or
5. install the camera on the objector's property (maybe while he is asleep or on holiday)– hard paternalism.

4.4.2.3 Individual

The application of surveillance with an appeal to paternalism for a justified cause in the individual case is easier to envisage if one thinks of how surveillance of a child or someone

of diminished responsibility might operate, and then applying this to the surveillance of a fully autonomous adult. Hence parents may give their children mobile phones with tracking devices on them so that the parent can always know the location of the child (or, at least, the child's mobile phone). Similar technology has been proposed in Norway for people suffering from dementia (Sandelson 2013). Accepting that at least some people suffering from dementia move in and out of moments of lucidity, those people would be mentally competent and autonomous to decide for themselves whether to agree to such tracking devices being placed on them during these periods of lucidity. To ignore their wishes expressed during moments of lucidity would therefore be to override their competent, autonomous choice.

In this scenario the carer of the patient who suffers dementia proposes the system to the patient, who is currently lucid and who opposes the idea. The carer's options are then as follows:

1. check that the patient is acting voluntarily and autonomously when he refuses the tracking system. If he is then the carer cannot install it on his phone – soft paternalism;
2. try to persuade the patient to install the system on his phone as it will make his (and his carer's) life a lot easier. If he is not persuaded, though, the carer cannot install it on his phone – rational non-interventional paternalism;
3. offer incentives to the patient to install the system on his phone. The carer will do extra housework if he installs it, or removing a privilege if he does not. Again, if he is not persuaded the carer cannot install it on his phone – incentive paternalism;
4. introduce a more subtle mechanism to encourage him to accept the system on his phone. Perhaps all of his friends with dementia have installed the same system, or maybe the system works as part of a game that allows him to "check in" to various locations automatically and compete with others to win prizes for being a frequent attendee at certain venues – libertarian paternalism;
5. install the system anyway, with or without his knowledge, and run it despite his opposition – hard paternalism.

4.4.3 Responding to Paternalism

Having looked at five different types of paternalism, ranging from soft to hard, and seen how these may be applied to surveillance, I am now in a position to offer a critique. Owing to the different types and different possible applications of paternalism, any response to its acceptability requires a more nuanced answer than may at first appear to be the case. One needs to ask, "what sort of paternalism is it and how is it being applied?" In this section I will develop my response to each of the five types of paternalism. In each case I will consider the response from the perspective of the state, the community and the individual as outlined above.

The first type of paternalism is Feinberg's soft paternalism. This is the case when the paternalist seeks to understand whether the agent is autonomous and acting in a voluntary capacity. I find nothing wrong in this soft paternalism, and even wonder whether it deserves the name paternalism, as does Feinberg (Feinberg 1986 p. 12). Rather it is an epistemic measure to determine whether or not the ensuing act would be paternalistic. If the agent is not autonomous or not acting voluntarily then the act would not be paternalistic. If, on the other hand, the agent is autonomous and acting voluntarily then to go through with the act would be paternalistic. However, given that the soft paternalist would not go through with the act on discovery of the latter he or she does not in fact act paternalistically. This is true whether the soft paternalist is the state, the community or an individual.

The second type of paternalism I described as being Savulescu's rational non-interventional paternalism. In this case the paternalist can argue for his or her case by presenting an argument in a rational and fair manner. In this case I take it that there must be sufficient information available to the agent. That is, the paternalist cannot withhold information and should inform the agent of any information that might argue against the paternalist's own position. Under these circumstances I do not see a significant problem with the rational non-interventional paternalist. Indeed, in a liberal democratic state it is typically by persuasion through rational argument that decisions are reached (or, at least, this is how decisions *ought* to be reached in liberal democracies). Similarly in communities founded upon some notion of a liberal contract there will likely be scope for rational discussion. If so, then the rational non-interventional paternalist is doing nothing wrong in stating his or

her opinion regarding the installation of the cameras. For the purposes of this thesis, I will assume that in communities in which there is no scope for rational discussion, such as religious or ideological communities suggested earlier, then the free entry and exit from those communities amounts to waiving one's right to autonomy in certain areas while a member of that community. If there is no such free movement out of the community then that community will be at risk of engaging in false imprisonment and so lose moral authority over the person imprisoned.

I do not see a problem in the case of the individual application of rational non-interventional paternalism, either. Once more, it is through discussion and consideration of competing opinions that rational, autonomous individuals should and often do arrive at their conclusions. This is laudable rather than problematic. To hold back on presenting an opinion and the reasons for holding it could deprive the individual from considering one particular perspective. Such self-censorship may be appropriate if it is feared that the person holding that opinion has undue influence over the individual such that he might arrive at a conclusion *simply because* this person held it. This would not (necessarily) be a rationally reached conclusion and so could undermine their ability to decide freely.

This is recognized by Savulescu when he accepts that any authority expressing its opinion as a rational non-interventional paternalist will typically carry a lot of weight in its argument simply by virtue of being an authority. We tend to listen to the opinion of a doctor or a lawyer over that of a lay person because we believe that they know what they are talking about. Similarly for many people, there is a likely tendency to agree to what the government says (or perhaps the political party they support) simply because it is the government (or the political party they support) without giving full attention to the details of the argument.

I accept that this is a problem for the rational non-interventionalist position and cannot see an easy response. It does mean that responsibility sits heavily on the paternalist's shoulders in this case to present as fair and honest an argument as possible, and to do his or her best to ensure that the agent has all the available information. It may be, as I have suggested, that there is a duty incumbent on the authority or perceived authority to be sensitive to the concerns of the individual making the decision and to exercise self-censorship where this

was deemed appropriate, and ensure that the voices of other, possibly dissenting, experts were also heard.

Beyond this concern I again think that it is excessive to describe the rational non-interventionalist as being paternalistic. It is quite normal and correct for the state to have to decide on a course of action and then, in a democracy, argue for that course in free and open debate. If the government wins the debate (i.e. brings people round to its way of thinking) then it can pursue its plans. Otherwise it cannot. This is similarly true of communities based on some form of liberal contract, and also of rational, autonomous individuals. This being the case I do not believe that the rational non-interventional position is paternalist.

Soft paternalism and rational non-interventional paternalism are not, I have argued, genuine cases of paternalism. This is because they continue to respect the autonomy and voluntary nature of the agents affected. These so-called paternalists may believe that a course of action is in the best interests of the agent but, if the agent is autonomous, rational and cannot be persuaded, both will ultimately bow to the will of the agent in areas of his best interest. This is not paternalistic (at least as I have defined it above). Furthermore, if the public, the community or the individual agrees to the surveillance then that entity is (broadly) consenting and so the surveillance does not require a justifying cause in the same way that non-consenting surveillance does.

The third type of paternalism I described was that of the incentive paternalist. The incentive paternalist goes further than the two so far considered in offering incentives and/or disincentives for complying with what she sees as being in the agent's best interests. Hence the incentive paternalist state may offer incentives such as tax breaks for those who comply, the community offer to pay for the cameras, or the wife may offer to cook every meal for her husband. Alternatively disincentives may be imposed, by the state through using fines for non-compliance, the community through ejecting the objector from a neighbourhood watch scheme, or the carer through removing a privilege from the patient with dementia.

Incentive paternalism involves greater interference than either of the previous two positions in that refusal to comply with the paternalist's perceived "best interests of the agent" may

carry with it a cost. The agent is hence technically free but not *totally* free in coming to a rational decision. His conclusions will be affected by the lure of the incentive or discomfort of the disincentive. How free the agent is will depend on a number of factors, including his baseline position (if he is impoverished then a small incentive could take on considerable weight) and the value of the incentive. With this in mind, in the case of individual surveillance whether or not incentives and disincentives are problematic will be affected by the baseline position of the individual and the value of the incentive.

Imagine that the community presses ahead with the installation of the cameras on all houses in the community except for Bob's house. If Bob's objection to the cameras was that he did not want to be subject to surveillance himself then his best option at this point may be to leave the community, although he can remain if he feels the cost of moving would be greater than the cost of being monitored. Bob maintains a certain freedom in the contractual nature of his relationship with the community which will involve costs and benefits as he compromises with the wishes of others in that community. Here it does not seem problematic for the community to offer to pay for the cost of Bob's camera. It does, though, seem heavy handed to threaten to eject Bob from the community for not complying. Having said that, there may be a concern that Bob is acting as a free rider on the public good provided by the cameras (Nozick 2001 pp. 90–95; Rawls 1999 pp. 96, 98). In this case, assuming that Bob is operating from the perspective of self-interest, it seems reasonable to provide Bob with an incentive to comply with the system or a disincentive to prevent his acting as a free rider.

In the case of the state engaging in incentive paternalism (and remembering that to clarify the distinction between paternalism and the tyranny of the majority I am assuming that all citizens who are not members of the government object to the surveillance) the distinction between incentives and disincentives remains pertinent, as does the problem of free riders once others begin to comply. However, the state does have a moral legitimacy in the use of coercion (and hence disincentives) which neither the individual nor the community necessarily possess. Because of this it may be more permissible for the government to use disincentives to encourage people to engage in activities which are perceived to be in the public's interest.

Libertarian paternalism challenges further the notion that the agent is free to decide. While incentives can affect the freedom of the agent in weighing the argument, the agent is at least aware of the incentives and can choose to disregard them. In the case of libertarian paternalism the mechanisms are not necessarily obvious as mechanisms (although, as noted above, they might be). As such, libertarian paternalism risks subverting the argument and attempting to secure people's compliance by means other than rational discussion. If this is the case then libertarian paternalism is manipulative and undermining of rational discourse.

Of course, influential factors other than rational considerations are frequently present in motivating discourse. Political discussions, for example, are frequently motivated by emotion in addition to consideration of the facts. However, to deliberately employ those factors rather than seeking to persuade through rational argument is bluntly disrespectful of the agent's autonomy. This being the case it is damaging to relationships between individuals, with one individual seeking to gain the upper hand through manipulation. At the community level it unfairly empowers one section of the community in getting their way even if that is not (or would not be freely) desired by all. At the state level, at least in liberal democracies, it is perhaps the most concerning as it threatens to undermine democratic intercourse. For a liberal democracy it is important that arguments are heard in order that rational decisions can be reached (Mill 1993 pp. 78, 83–123).

These arguments, though, are not necessarily the case in reality. As noted, this is a *risk* of libertarian paternalism. It is feasible that mechanisms are employed alongside rational discourse and are applied through consensus. However, if the mechanisms are employed with consent then this will not be, in my opinion, a case of paternalism. Rather this would be a matter of consenting to a certain structuring of particular goods in society such that the better is more likely to be chosen than the worse. The consent means that the act is not paternalistic. To be paternalistic in the manner I have been describing is to go against the will of the mentally competent, autonomous adult who is affected. Thus although libertarian paternalism may be acceptable, in such cases as it is (i.e. when consent is sought) it ceases to be genuine paternalism.

Similar problems arise with hard paternalism as with the risk of libertarian paternalism just discussed. In this case the state, community or individual makes no attempt to recognize the autonomous will of the agent but chooses to override their decision. There is in hard

paternalism, a strong sense of *immediate* disempowerment for the agent, and this is what is at heart wrong with it. Feinberg argues, "it says in effect that there are sharp limits to my right to govern myself even within the wholly self-regarding sphere, that others may intervene even against my protests to 'correct' my choices and then (worst of all) justify their interference on the ground (how patronizing!) that they know my own good better than I know it myself. It is that 'justification' that is most unpleasantly analogous to parental behaviour" (Feinberg 1986 p. 23). If Feinberg is correct in his assessment, then to be put into the role of a child before another person is immediately disempowering: no ground is offered to respond or resist. In this way, hard paternalism involves a seizing of power over another person such that equality with and the dignity of that person are ignored. Of course it is not unreasonable to allow the state to disempower a person through arrest and imprisonment who has done something wrong. However, in this case the autonomous agent under consideration has done nothing to make themselves liable.

It is only with the fourth and fifth types of paternalism that I believe there *necessarily* exists a genuine concern. I have argued that soft paternalism is a misnomer insofar as it is not really a paternalist position at all. Rational non-interventional paternalism and incentivizing paternalism may be slightly more problematic in cases where the argument of the authority may have disproportionate weight merely because it is presented by that authority, but this need not be the case. Libertarian and hard paternalism (as long as libertarian paternalism genuinely is paternalistic and not consenting) are always wrong in choosing to over-ride the voluntary and autonomous decision taken by people in order to implement the course of action the paternalist sees as being in the people's best interests. However, there remain some difficult cases which need to be addressed. These can be described as morally reprehensible acts which are entered into freely, and can be seen as offering a strong challenge to the anti-paternalist position that I have taken here.

The position for which I have argued so far leaves open the possibility that individuals may agree to enter into acts which are commonly seen as morally reprehensible, such as cannibalism or gladiatorial combat. In Germany in 2001 two men (Armin Meiwes and Bernd Brandes) who had connected over the internet met, removed, cooked and ate a part of Brandes' body. Meiwes then killed Brandes, at the latter's request, and ate him (Harding 2003b). The case is simplified if we imagine that, hypothetically, Brandes took his own

life. In this situation, two apparently autonomous individuals engaged voluntarily in an act which most would find reprehensible but which did not harm a third party. The paternalist would have no problem intervening and stopping this from happening. My own position, though, demands that I could at most seek to persuade and offer incentives to people not to engage in these activities.

A similar scenario is suggested by Irving Kristol and taken up by Feinberg (Feinberg 1988 pp. 128–129). Imagine, says Kristol, gladiatorial combat similar to those of the Colosseum in Rome taking place in Yankee Stadium. Feinberg admits that the initial response to this, even by an anti-paternalist, is likely to be that yes, there may be a problem here. However, he continues, the anti-paternalist should not concede ground so readily. One option would be to question the mental state and voluntary nature of both involved in the combat. This would be tantamount to the soft paternalist position. If either combatant were not acting fully autonomously or were in some way being coerced then the combat should be prevented. This though, accepts Feinberg, may be overcome by Kristol stipulating that both participants are fully autonomous, mentally competent and acting voluntarily.

A second response could be to accept that there are limiting extremes in which intervention may be justified, but that these are so far from the typical scenarios discussed in public (regarding pornography, gambling, soft drugs, etc.) as to be of academic interest only. This, though, Feinberg admits, may feel uncomfortable to the anti-paternalist. A third position would be to question the sort of society which would allow or result from the public attending such events. Such a society would be violent and brutalized, and legal coercion could at best "only treat the symptoms and slow their spread" (Feinberg 1988 p. 132).

To the third position Kristol may respond that, again, he wishes to stipulate that the scenario is such that the spectators and society at large are not affected one iota by this event. The problem with this, Feinberg rejoins, is that the scenario is now so far removed from reality that the initial intuition is considerably weakened (Feinberg 1988 p. 133). Indeed, given this situation it seems quite reasonable for the anti-paternalist to "boldly insist…that the law be kept from interfering, and thereby reject the force of the story as a counterexample" (Feinberg 1988 p. 329).

Returning to the case of Meiwes and Brandes both men were described as "disturbed", and Brandes in particular as "suffering from a severe psychiatric disorder" (Fickling 2006; Harding 2003b). As such, in the actual case interference would be acceptable. A soft paternalist would discover that neither man was fully mentally competent and so intervention would be part of a duty of care to both. This, then, is similar to Feinberg's first response to Kristol. However if, as with Kristol's gladiator example, the case is abstracted to two men who are not disturbed and are not suffering from any disorder, living in a society which would not be affected one iota by their actions, then the soft paternalist would allow the act of cannibalism to continue.

I am prepared to bite this particular bullet and agree that the cannibalism, like gladiatorial combat, should be tolerated. In practice I strongly doubt that such cases could ever exist without at least one of the parties being less than fully mentally competent, or without society being negatively impacted in such a way that more people would be harmed than merely the participants, and so in practice I believe that intervention would probably always be permissible. I am wary, though, of merely reclassifying actors engaged in morally reprehensible acts as "less than fully mentally competent." It would beg the question if someone who engaged in a morally reprehensible act were defined as less than fully mentally competent. Because of this I am, as I say, prepared to bite the bullet and accept that in cases where full mental competence can be demonstrated, along with autonomy and voluntary action, consensual morally reprehensible acts should be tolerated.

4.5 Conclusion

In this chapter I have argued that there is a need to provide a just cause when seeking to justify acts of surveillance. This justified cause can be grounded in liability, in which a person's decisions or actions warrant them being subjected to the harms of surveillance in order to apprehend the person or prevent the actions. It may also be grounded in justifiably treating a person or people as liable if there is sufficient reasonable evidence that a person or people may be involved in decisions or actions that would render them liable for surveillance. Thirdly, I argued that the existence of significant benefits, coupled with minimal harms, as is the case in the surveillance of passengers in a public transportation network, can also provide a justified cause. Finally I considered paternalism as a possible grounding. Here I argued that provided that the paternalist did not over-ride the voluntary,

autonomous will of the agent then it was not problematic. At the same time, surveillance that did not do this would be consenting surveillance and so not require a justified cause in the same way as non-consenting surveillance. I also argued that libertarian and hard paternalism, which do over-ride the voluntary and autonomous will of the agent, cannot be used to justify surveillance.

5. Intention

Imagine a young woman walking down a street. She is wearing a short skirt and a loose-fitting blouse. Above and unbeknownst to her, a pan-tilt-zoom (PTZ), CCTV camera follows her as she walks. Imagine now the scene inside the CCTV operations centre. A middle-aged male operator uses a joystick to remotely control the camera and follow the young woman. He is able to zoom in and fill his monitor with an image of her face or her body.

Is there anything wrong with this picture? With the information given it is very hard to say. However, it seems at least reasonable to question the intentions of the operator as he follows the woman from a distance. It may be that the operator finds himself attracted to the woman. He notices her in a crowd, and purely because of the attraction zooms his camera in on her and follows her as she walks. He may know her or he may not. This may be the first time he has seen her through his camera, or he may have been tracking her over a network of cameras whenever she came within the camera's "gaze" for some time. In any case, the sole reason for his focussing the camera on the woman is this attraction. There is little to distinguish between the camera operator and a stalker, other than the fact that the operator is separated from the subject of his attention by the camera, and so perhaps less likely to be caught (and perhaps also less likely to cause distress or make her feel harassed).

This, though, is not the only story we could tell. It may be that the operator thinks that he has seen this woman's face before. Not as an object of attraction but as a photograph among a list of suspects for a recent terrorist bombing. Through following her and zooming in on her face he is able to increase his chances of determining whether or not she is that suspect. Such identification may come through a likeness of the facial image, or further information regarding her gait or some other identifying aspect of her person.

While there may be other factors in a real world situation, the significant difference between these two cases, the first of which I shall call "Stalker" and the second "Hero", that I will consider in this chapter is the intention of the operator. In the case of Stalker the intentions of the operator are base. In Hero, on the other hand, the intentions of the

operator are nobler. He is not following the woman because she is attractive, but rather because he is concerned that she may be a threat to public safety.

In this chapter I examine the moral relevance of intention, which underlies the difference between Stalker and Hero. Drawing on the use of "correct intention" as a principal in the just war tradition I argue for the moral importance of an actor having the right intention in surveillance. I then consider some significant objections to the moral relevance of intentions as put forward by Thomas Scanlon. I will reject Scanlon's objections and argue that it is correct to include intentions as a means of morally assessing the permissibility of an act of surveillance.

To those not familiar with the debate, the claim that intention is morally relevant to the ethical justification of either war or surveillance might appear to be uncontentious. In criminal law the relevance of intention is recognized in the difference between, for example, murder and manslaughter, with different lengths of incarceration resulting from each. Similarly in war, we accept that tragic accidents do happen. If it transpires that what was at first believed to be an accident was in fact intended, though, we are outraged and demand justice of the perpetrator. In these cases of killing and war the distinction is between intention and no intention (or intention and accident). There is a separate issue, though, regarding the quality of the intention. That is, does the *sort* of intention matter? Imagine that I intend to do X but foresee that Y will also result directly from my doing X. Is there a morally significant difference, then, between my intending to do X and foreseeing Y and my intending to do Y and foreseeing X? In both cases X and Y will result, the only difference is which of the two I intend to happen as opposed to merely foresee.

5.1 The Moral Relevance of Intention in War

5.1.1 Soul of the Perpetrator

In the just war tradition, correct intention was identified as being of major importance by Augustine of Hippo (Augustine 2006 pp. 83–84). This importance was agreed by later writers such as Raymond of Peñafort and Thomas Aquinas (Penafort 2006 p. 135; Aquinas 2000 pp. 1353–54). It has continued to remain a major principle in the just war canon as discussed by Elizabeth Anscombe and the Roman Catholic Bishops of America (Anscombe

2006 p. 632; National Conference of Catholic Bishops 2006 p. 673). In these writings there are two considerations of intention. The first is for the sin of the perpetrator or agent. If the agent has a poor, or incorrect intention, then he is putting his soul at risk, which is bad either because it could lead to eternal damnation or because the soul is inherently valuable and should be protected.

Put in less theological terms, people (as opposed to God) tend to judge a person's moral conduct by that person's intentions rather than by the justifications that person is able to give for acting. Many can give good reasons for acting, but if it transpires that they had an ulterior motive for acting in the way that they did, and that ulterior motive is not justified, then they will be judged for the intention rather than the reason provided in the first instance. Hence to act with an incorrect intention risks exposing the actor to the disapproval of her peers and/or it can risk damaging her (inherently valuable) character.

The concern with the soul of the perpetrator is apparent also in the scenario of Hero and Stalker. Even though I have stipulated that their actions are the same, I have suggested that the Hero is justified in his actions while the Stalker is not. This is because Stalker, unlike Hero, has incorrect intentions regarding the woman who is being watched. There is no justified cause for watching her with the intentions that Stalker has in mind (i.e. personal gratification rather than public safety). Were Stalker's intentions broadcast to his peers they would be understandably disapproving. Whether such voyeurism is damaging to the inherently valuable character of Stalker is an empirical claim which would have to be tested, but my suspicion is that it would have some negative impact.

To illustrate this, take Stalker as being similar to a peeping Tom. The traditional image of the peeping Tom is of someone who peers in through parted curtains to watch someone else undressing, when the surveilled subject is unaware of the surveillance. A more contemporary picture may involve the peeping Tom using sophisticated equipment such as telephoto lenses or even remote-controlled cameras such as Stalker. Clearly there are many problems with this scenario. Given the current consideration of intention, though, one must question what the illicit gaining of such knowledge and/or images will do to the virtue of that individual. There is, I would suggest, a suspicion that peeping Toms are not examples of well-adjusted individuals. That is to say, there is already something wrong with a person who would willingly violate another's privacy for their own personal kicks. If this is true

then the surveillance by the peeping Tom is the evidence of an imbalance in the peeping Tom's own moral character. Furthermore, the response that society typically has to peeping Toms (normally some form of punishment) demonstrates a social disapproval of this behaviour. As such, both concerns listed above (exposure to disapproval and damage to character) are fulfilled in the case of peeping Toms.

As I shall show, Scanlon does not dispute this, although he does argue that it has relevance only for the decision process made by the person and not for the justification of the act. The person in choosing to commit the act has thus made a worse decision than one who does not so choose, but this has no impact on the permissibility of the act itself (Scanlon 2008 pp. 23–26).

5.1.2 Impact on Outcomes

The second consideration is that of effects. If the agent has an intention which is at odds with the stated cause, then it is possible that more damage will likely occur as a result of that agent's actions. Anscombe argues that the cause of the Allies' fighting in the Second World War was to defeat Hitler. However, their intention of demanding total surrender was to some degree at odds with this cause because total surrender was not necessary to defeat Hitler. Indeed by demanding such, she argues, the Allies were prolonging the war by denying the Axis powers hope for a face-saving means of leaving the war. This being the case, the Axis powers were likely to continue fighting for as long as possible (Anscombe 2006 p. 632).

Anscombe's argument as it stands is contingent, though. She is correct in this case that the intention (total surrender) differed from the cause (defeating Hitler) and that this led to a different outcome than had the intention been the same as the cause. However, it seems plausible that the intention may differ from the cause in the opposite direction. Hence the cause of the war may be so heinous that it justifies a demand of total surrender, yet the intention, in seeking to limit loss of life, is to pursue a limited surrender. What Anscombe's argument does demonstrate, though, is that in cases where intention differs from cause it is necessary to assess each individually. That is to say, intention is significant in the ethical assessment of the war as it can lead to different outcomes from the cause.

Once more this consideration can be illustrated in the case of surveillance with the Hero and Stalker scenario. Imagine that cameras have been installed in public places with the purpose of capturing criminals. In this case the effects of Hero's surveillance are easier to predict as his intentions mirror the justifying cause. He will look for and focus on likely criminals, such as he imagines the woman to be. Stalker, by contrast, will not always be looking for likely criminals, at least while he is watching the woman. As a result, a known criminal could pass under his gaze without him realizing. Furthermore, if his intentions ever became known, this could lead to a significant number of people experiencing the sense of being "undressed by the eyes" of an unknown watcher every time they pass before a CCTV camera.

Scanlon would likely not disagree with this argument. His response could be that in such cases the effects *are* different as a result of the intention (he refers to this as the "predictive significance of intent" (Scanlon 2008 p. 13)), but that it is the effects that are morally relevant, not the intention. He carefully constructs thought experiments for consideration in which the intentions differ but the outcome is identical. To properly assess Scanlon's *philosophical* claims, then, it is important to consider the cases he proposes in which the effects remain the same while the intentions differ. Nonetheless, if this argument is to have any impact outside an abstract thought experiment then the possibility of differing intentions having differing outcomes in real world cases is an important consideration in determining why intentions are relevant in such cases.

5.1.3 Smokescreens

To these considerations I would suggest a third, illustrated by a more contemporary example. In 1991 Saddam Hussein commanded the army of Iraq to invade Kuwait. The international community, led by the United States, responded by stationing troops in Saudi Arabia and then entering Kuwait to expel the Iraqi forces. At the time one argument made against the fighting focussed on President George Bush Senior's desire to secure the oil fields of Kuwait and Saudi Arabia from hostile occupation, summed up in the slogan "no blood for oil". In this argument the claim was made that Bush had an ulterior motive for entering Kuwait. While he *claimed* legitimacy in declaring war on Iraq as a response to an illegal occupation, the argument's proponents held that his intentions lay elsewhere. As such Bush was being portrayed as raising a smokescreen. He claimed an ethical rationale

for his actions, but used this as a smokescreen for his (less ethical, at least in the eyes of his critics) intentions.

It is worth noting that the presence of a smokescreen, hiding genuine intentions behind justified causes, implies that the outcome will be worse than if the cause is the sole motivating factor for the war. If the outcome, given the genuine intentions, would be better or the same as if the justifying causes were the sole motivating factor then there would be little or no need for the smokescreen.

As such the existence of smokescreens is indicative of ulterior intentions which, as argued above, can have an impact on outcomes. The smokescreen itself, though, is an act of deception. It is a deliberate act of lying in an attempt to deceive the people at whom it is aimed. Given that lying is almost universally recognized as unethical, it is reasonable to conclude that smokescreens, at least as I have presented them here, are also unethical.

As with the consideration of impact on outcomes, I do not think that Scanlon would have a problem with this argument. As with those cases, his response would likely be that this has a direct impact on outcomes and so does not reflect the nature of the cases he is challenging. In response to the accusation of lying his argument suggests that he would accept that the decision to deceive was a bad decision, but that this does not affect the permissibility of the action itself. It is, he holds, only when outcomes are identical and intentions differ that we can determine the extent to which intentions are morally relevant to the permissibility of an action.

5.1.4 Inherent Value

The fourth consideration is the inherent value of intention. Independent of consequences, it seems intuitively reasonable to believe that intentions are important in and of themselves. This is a strong intuition and it is this that Scanlon acknowledges and seeks to challenge (Scanlon 2008 p. 18). His argument is that if he can present cases in which intention is clearly not morally relevant to the permissibility of an action then he will have demonstrated that intention is not inherently valuable. Its value is rather instrumental, as outlined above.

In the remainder of this chapter I shall test the intuition of the inherent value of intention against Scanlon's cases and accompanying arguments. I shall argue that his position is untenable and that his objections to the intuition that intention is inherently valuable fail. As such I believe that the intuition is correct, absent a stronger defeater than Scanlon has so far presented.

5.1.5 Conclusion

I have argued that there are four reasons why correct intention matters in war. The first is the consideration of the perpetrator's soul. With a malign intention the perpetrator risks eternal damnation, damage to an inherently valuable aspect of his character, or at the very least the condemnation of his peers. The second consideration is that of the effects of the war. If the intention is other than the cause then the outcome of the war could be different than if the intention and cause were the same. The third consideration is that the cause may be used as a smokescreen for less ethical (or unethical) behaviour. The presence of a smokescreen is indicative of lying, which is wrong. The fourth consideration is the inherent value of intention in determining the permissibility of an action.

It is noteworthy that Scanlon would likely accept each of the first three considerations as having an impact on the permissibility of an act. However, his likely counter would be that the impact is relevant only to the actor and not to the permissibility of the act itself (as in the concern regarding the soul of the perpetrator and his using smokescreens as deception); or that the impact is indirect (through affecting outcomes either directly or as a smokescreen). In none of these three cases, then, would Scanlon seem to have a problem. It is with the fourth consideration, the inherent value of intention, that Scanlon takes issue and focuses his argument.

It is now time to consider Scanlon's arguments in greater depth to see how he challenges the moral relevance of intention and whether he is successful in this. Scanlon's arguments are written in the context of the moral relevance of intention as a factor in the doctrine of double effect, but for our purposes there is no significant distinction between the relevance of intention in such double effect reasoning and the relevance of intention elsewhere in just war deliberations. Scanlon states that "the question I am interested in is whether an agent's intention is itself *directly* relevant to the permissibility of an action [emphasis added]"

(Scanlon 2008 p. 13), and again, "to my knowledge no one has come up with a satisfying theoretical explanation of why the fact of intention, in the sense that is involved here – the difference between consequences that are intended and those that are merely foreseen – should make a moral difference" (Scanlon 2008 p. 18). It is because of Scanlon's focus on *direct* relevance that the considerations above need to be set aside in considering his critique. Once more, they are relevant in real world cases as to why intentions should matter, but not in the hypothetical scenarios that Scanlon constructs.

5.2 Scanlon's Argument against the Moral Relevance of Intention

Scanlon bases his critique on what he sees as the dual use of moral principles. One use is critical, in which the moral principle is employed to assess the decision-making process of an agent. This he distinguishes from Judith Jarvis Thomson's use to assess the character of an agent, stating that, "what is being assessed is not the agent's overall character but rather the quality of the particular piece of decision making that led to the action in question" (Scanlon 2008 pp. 27–28). As such, the critical use of a moral principle can tell us whether an agent made use of a good or bad decision process, and therefore has a relevance in attributing blame to the agent if he or she was found to have ignored factors which should have been taken into consideration when deciding on a course of action. Hence one's "criticism of the way an agent decided what to do is unavoidably predicated on assumptions about the agent's state of mind - in particular about what he or she took into account in deciding what to do and took as reasons for and against acting as he or she did" (Scanlon 2008 p. 23).

The other use of moral principles is deliberative and comes of asking, "which considerations do, and which do not, count for or against various courses of action" (Scanlon 2008 p. 23). This assessment is of the action itself, rather than the agent's decision-making process, and asserts whether the action is right or wrong. Whereas the critical use is relevant in attributing blame, the deliberative use is relevant in assessing the permissibility of the act. Putting these in the context of Hero and Stalker, the act of watching the woman over CCTV is either permissible or not, and the intention of the operator has no bearing on this (i.e. it is a deliberative consideration). By contrast, the decision process of Hero is good whereas the decision process of Stalker is bad (i.e. a critical consideration) and so we attribute praise to Hero and blame to Stalker. Hence

Scanlon states, "what makes an action wrong is the consideration or considerations that count decisively against it, not the agent's failure to give these considerations the proper weight" (Scanlon 2008 p. 23). In looking at those considerations, Scanlon argues that they should be weighed against one another such that permissibility is ultimately decided by considerations of proportionality, qualified by a recognition of relevant rights and duties (Scanlon 2008 p. 35).

To demonstrate this distinction between the use of moral principles as critical and as deliberative, Scanlon draws on a number of illustrations. I shall use just two of these here, each drawn from Thomson (Thomson 1992 p. 229), as they are sufficient to demonstrate Scanlon's argument fairly and without repetition. The first of these I shall call PMC for Prime Minister and Commander. It draws upon a scenario in which a pilot is sent to drop a bomb on a munitions factory in the knowledge that the explosion will kill non-combatants in the vicinity of the factory. It is often taken to be the case that the pilot would be justified in dropping the bomb if his intention were to destroy the factory, but not if his intention were to kill the non-combatants. In the acceptable case the bomber's intentions are pure, and he is typically referred to as the Strategic Bomber (SB), while in the unacceptable case the bomber's intentions are wrong, and he is referred to as the Terror Bomber (TB). However, Scanlon begs to differ on this point:

> Suppose you were prime minister, and the commander of the air force described to you a planned air raid that would be expected to destroy a munitions plant and also kill a certain number of civilians, thereby probably undermining public support for the war. If he asked whether you thought this was morally permissible, you would not say 'Well, that depends on what your intentions would be in carrying it out. Would you be intending to kill the civilians, or would their deaths be merely an unintended but foreseeable (albeit beneficial) side effect of the destruction of the plant?'…I agree with Thomson in finding this implausible (Scanlon 2008 pp. 19–20).

The second illustration is of a doctor offering pain relief to a patient, which we shall hereafter refer to as PRD for Pain-Relieving Doctor:

> Suppose that a patient is fatally ill and in great pain. The only course of medication that will relieve this pain will also cause the patient's death. Suppose that the patient wants to be given this drug. Does the permissibility of administering it depend on the doctor's intention in doing so - specifically, on whether the doctor intends to relieve the pain by causing the patient to die or intends to relieve the pain by giving the drug, which will, inevitably, also cause

> the patient's death? Thomson says, plausibly, that it does not (Scanlon 2008 p. 19).

In PRD Scanlon accepts that a murderous doctor would be a bad person, but holds that it is still better for the patient to have the pain relieved. "If [the doctor] is moved by such reasons, then she is a morally bad person. But it does not follow that it is impermissible for her to administer the drug (or that the patient should have to wait until a different doctor, with better intentions, comes on duty)" (Scanlon 2008 pp. 19–20). Hence the action (the relief of pain) is permissible even though the agent (the murderous doctor) is blameworthy.

Drawing from his discussion of the dual use of moral principles, Scanlon concludes that an agent's intention is (or at least may be) relevant in assessing that person's decision-making process, but not in assessing the permissibility of the action itself (except to the extent that it may have an impact on the outcome, as discussed above). Furthermore, in looking at the various cases he notes a degree of similarity between them, in that "although the examples differ in many ways, they all have the same structure: they concern general principles that sometimes admit of exceptions, and they raise questions about when those exceptions apply" (Scanlon 2008 p. 25). Finally, in his discussion of these similarities he determines that proportionality, qualified by an appreciation of rights and duties, is a good guide to permissibility (Scanlon 2008 p. 35). For the remainder of this discussion I shall refer to this belief that permissibility should be determined by proportionality qualified by recognition of certain rights and duties as Scanlon's General Principle.

5.3 Response to Scanlon's Argument against the Moral Relevance of Intention

In responding to Scanlon's critique I offer two arguments. The first, drawn from McMahan, concerns the scope of moral responsibility, and holds that while we may not be responsible for each other's decisions, we are nonetheless responsible for our own (McMahan 2009). Furthermore, the perspective that is described will determine the scope that is under consideration in a particular context. The second is that some acts are by their very nature intentional. It is therefore impossible to separate out the act from the intention in the way that Scanlon claims. As a result of the two arguments I argue that Scanlon fails to establish the irrelevance of an agent's intentions to an act's permissibility.

5.3.1 First Argument

The first argument in response to Scanlon holds that he overlooks the role of scope in his examination of moral scenarios, and that scope will be determined by the perspective under consideration. For the sake of this argument I shall accept Scanlon's positing that it makes no difference to the person who is killed whether their life is taken by a well-intentioned or poorly-intentioned person. I shall start by looking at PMC but then turn to PRD to show that this problem is not limited to military cases.

In PMC Scanlon asks the reader to think of herself as the prime minister considering a bombing raid proposed by the commander of the air force. When the commander suggests bombing a munitions plant in a raid which would also kill non-combatants it is suggested that the reader, as prime minister, would not ask the intention of the commander conducting the bombing raid. In a later discussion of a similar scenario Scanlon argues that, "it seems clear that your answer should depend on whether, given the likely consequences of the strike, there is a justification for it that meets the relevant criteria. You should not say, 'Well, it depends on your intentions'" (Scanlon 2008 p. 31).

Scanlon's response here is problematic. The issue in question is to ascertain the relevant criteria, and whether intention is one such criterion. As the picture stands, I am not persuaded. I believe that, on the contrary, the intentions of the commander are a highly relevant consideration insofar as his planned raid might commit the state to a morally reprehensible act.

Imagine that the commander is called in by the prime minister to discuss the scenario laid out in PMC. The prime minister discusses the munitions plant with the commander, and the thorny problem of there being a number of civilians in the immediate vicinity. Imagine now that the commander responds to the effect that he actually enjoys killing the civilians. In fact, he says, he would *prefer* to target the civilians than the munitions plant, but he acknowledges that this goes against those pesky rules of combat and so realizes that the best way to kill the civilians without incurring international condemnation is to aim for the munitions plant. This way the prime minister gets what he wants (the destroyed munitions plant), the commander gets what he wants (lots of dead civilians) and the international community does not have to get involved.

It would be bizarre in this modified version of PMC to suggest that the prime minister would think that the commander should go off and carry out the bombing given what he has just said. He would be more likely to strip the commander of his authority and put a different person in his place. I struggle to think of anyone who, upon hearing this if they were the prime minister, would respond, "That is fine, Commander, all I care about is the munitions plant; your intentions are irrelevant to me." If I am correct in this, then the reason that Scanlon's scenario works is not because the commander's intentions are irrelevant to the prime minister, but because they are unknown to the prime minister. Once they become known, the reaction of the prime minister should be obvious.

Even if the reader disagrees as to how the prime minister would react, the thought experiment does *not* establish the irrelevance of the commander's intentions to the permissibility of the act, as Jeff McMahan has pointed out. However, it does establish the irrelevance of the commander's intentions *to the prime minister* (McMahan 2009). This is because the prime minister is (morally) responsible for his own intentions in the areas for which he is (practically) responsible, such as determining policies for the prosecution of the war. The intentions of the commander of the air force fall outside the scope of the prime minister's moral responsibility, and so they are not a relevant consideration for him. The prime minister is not the commander's moral conscience.

On similar grounds, the commander of the air force is not morally responsible for the policies set by the prime minister. He can choose whether or not to implement these policies, for it is in the realm of implementation that he has some control and hence it is over this realm that his moral scope extends. If the prime minister creates a new and morally reprehensible policy, such as carpet-bombing civilians, the commander can refuse to implement it for moral reasons. If, on the other hand, the commander chooses to implement it then he is held morally responsible for this decision and its consequences, but he cannot be held responsible for the policy itself. Thus it is the areas over which one has control that one has moral scope, and thus moral responsibility (McMahan 2009).

Moving on to the PRD scenario, it will be recalled that the patient is in need of pain relief which will lead to his death. Scanlon asserts that the intentions of the doctor are irrelevant to the patient, who simply wants relief and does not want to wait for a doctor with good intentions to do the rounds. Scanlon here makes a good point that if we consider the

situation from the perspective of the patient then the intentions of the doctor make little difference. Indeed, the outcome from the patient's perspective will be the same in either case by the very nature of the scenario, and it is the outcome which interests Scanlon the most. He writes, "what are of fundamental relevance in these cases are the *effects* of the agent's action on the world around her (or what it is reasonable to expect those *effects* to be) [emphasis added]" (Scanlon 2008 p. 13), and again that, "the intention is wrongful because the act intended is wrongful, and the act is wrongful because of its likely consequences, not (fundamentally) because of the intention" (Scanlon 2008 p. 29). If that which makes a moral difference is the outcome of an action, and the outcome is the same no matter the intention, then there will be no moral difference. However, this is not the whole story.

If we consider PRD from the perspective of the *doctor* a very different scenario emerges. Scanlon is correct in asserting that the doctor has made a bad decision, but more than this, in intending to kill the patient the doctor has from her (the doctor's) perspective made a wrong decision. It is simply not permissible for doctors to desire to cause death, even if they can offer excuses for their actions. To see this, imagine Orin Scrivello, the dentist portrayed in the *Little Shop of Horrors* (Oz 1986). As a sadist, Scrivello enjoys causing pain to his patients and is frustrated when masochistic patients who enjoy being hurt enter his surgery. Take a scenario now in which a patient has some condition, the treatment of which is imminently necessary and will cause considerable pain whoever the dentist. As the patient sits down in Scrivello's chair, the dentist leans over with a grin and says, "This is going to hurt, you know. But that's alright, because I enjoy your pain." To even say this would be, at the very least, unprofessional. Knowing that it is true, though, I contend that Scrivello should be struck off from practicing as a dentist. While it may be a joke in musical comedies, the idea of a genuinely sadistic dentist is disturbing. I suggest that we generally believe that dentists should both act to relieve pain *and* desire to relieve pain.

Similarly, it seems to me that doctors who want to kill their patients, rather than relieve them of pain, are antithetical to what society believes a doctor should be. Such doctors should be struck off the medical register and forbidden to practice, even if the effects of their actions are the same as beneficent doctors. It is therefore relevant to ask whether the

doctor intends the easing of pain or the causing of death, for one of these is permissible while the other is not.

If therefore we follow Scanlon in looking at just the (likely) effects of an action on the patient to assess that action's permissibility we may well judge the intentions of the agent to be irrelevant. If, on the other hand, we consider permissibility from the perspective of the agent then we may reach a different conclusion.

Scanlon's argument therefore gains credence by reducing the information available to the prime minister/patient and by limiting the focus of the reader's attention to the perspective of just one of the agents when there are in fact two agents whose perspectives need to be taken into account. Through focussing on the prime minister (PMC) and the patient (PRD) Scanlon argues that these agents need not care about the intentions of the commander or the doctor respectively. I have challenged this in two ways. Firstly to say that were more information available to the prime minister or the patient then their reactions would be entirely different from how Scanlon suggests. Secondly, if I am wrong in this assertion and Scanlon is correct in his assessment of their reactions, there is a further problem. As demonstrated by McMahan, Scanlon does not demonstrate the irrelevance of intention to permissibility of the action, but rather the irrelevance of intention *to* the prime minister or the patient.

5.3.2 Second Argument

My second argument holds that some acts are intentional by definition. Targeting a person to kill them (i.e. placing them in the sights of a gun or missile) is such an act. One cannot "unintentionally" target a person simply because the definition of targeting a person in this manner holds within it the intention to kill or at least hurt that person.

It may be objected that the pertinent distinction is not between "intended" and "unintended" targeting but between "intended" and "merely foreseen" targeting, the point being that there is a difference between unintended targeting and merely foreseen targeting. In this case I hold equally that one cannot "merely foresee" one's targeting of a person any more than one can "unintentionally" target a person. One *can*, by contrast, unintentionally kill or merely foresee the killing of another person.

Killing another is therefore qualitatively different from targeting another. Killing can be carried out unintentionally or be merely foreseen. Targeting cannot be carried out unintentionally or be merely foreseen: it requires intention.

When it comes to targeting in war then, the pertinent question becomes who is it that the soldier intends to kill? This is best examined by looking at the just war principle of discrimination. Through this I will demonstrate how Scanlon's attempts to avoid the moral relevance of intention leave his argument in an untenable position.

The importance of targeting, as opposed to killing, is central to the traditional just war principle of discrimination. This concerns the differing treatment one should afford to combatants and non-combatants in war. In writing on this principle Francesco di Vitoria, a leading thinker in that tradition, offers a comprehensive definition that grounds the principle rather than merely stating it. He writes:

> First, *it is never lawful in itself intentionally to kill innocent persons*. This is proved, in the first place, by Exodus 23:7, where it says "the innocent and righteous slay thou not". Second, the foundation of the just war is the injury inflicted upon one by the enemy, as shown above … ; but an innocent person has done you no harm. *Ergo*, etc. Third, within the commonwealth it is not permissible to punish the innocent for the crimes of the evil, and therefore it is not permissible to kill innocent members of the enemy population for the injury done by the wicked among them. Fourth, the war would otherwise become just on both sides, since it is clear that the innocent would also have the right to defend themselves. All this is confirmed by Deuteronomy 20:10-20, where the children of Israel are commanded, when they have captured a city, to smite every male thereof with the edge of the sword, but to spare the women and the little ones (Vitoria 2006 p. 324).[7]

By contrast, Scanlon seems to take the prohibition to be against *killing* non-combatants. This can be seen if we look at his argument concerning the principle of discrimination:

> In war, one is sometimes permitted to use destructive and potentially deadly force of a kind that would normally be prohibited. But such force is permitted only when its use can be expected to bring some military advantage, such as destroying enemy combatants or war-making materials, and it is permitted only if expected harm to

[7] To avoid an appeal to authority we may strip out the biblical references provided by Vitoria. In this case, though, there are still three reasons given for the principle of discrimination, namely that an innocent has inflicted no harm; that the innocent should not be punished for the crimes of the guilty; and that the war would be just on both sides as the innocent would be justified in acting in self-defence. In each of these cases the prohibition is on *intentionally* killing innocents and not on killing them *per se*.

> non-combatants is as small as possible, compatible with gaining the relevant military advantage, and only if this harm is "proportional" to the importance of this advantage (Scanlon 2008 p. 28).

It is not clear here whether Scanlon is offering an alternative definition of the principle of discrimination or a rephrasing of the principle in terms of proportionality in which combatants and non-combatants are given different weights. If we take it to be the former then it is a curious alternative. Despite the principle of discrimination being a long-held tenet of the just war tradition, Scanlon does not offer a source for his definition. This would be acceptable if he offered a justification for the alternative definition, but he does not do this either. He is therefore neither grounding this definition in the traditional discourse nor offering grounds to prefer it to that given in the traditional discourse.

Rather than offering a new definition of the principle of discrimination it may be that Scanlon is rephrasing it in order that he can maintain the principle in such a way as to avoid intention being relevant to the principle. Hence he writes that provided the "harm to non-combatants is as small as possible" and if this harm is proportional to the relevant military advantage, then the harm-inducing action is permissible. Unlike Scanlon's General Principle, this is not a rule admitting of rights or duties which *cannot* be breached by considerations of proportionality. Rather the rule amounts to nothing but two considerations of proportionality (military advantage and reduction of harm). The problems in Scanlon's version of the principle of discrimination become clear when Scanlon attempts to explain why it is that SB might be permissible and TB impermissible:

> If there is no munitions plant, but a bombing raid that would kill the same number of non-combatants would hasten the end of the war by undermining morale, this raid (a pure case of "terror bombing") would be not permissible… It is impermissible because it can be expected to kill people, and the circumstances do not provide a justification for doing this under the principle just stated. The death of non-combatants is not rendered a "military advantage" by the fact that it would shorten the war by undermining public morale. So the fact that it would do this does not bring the case under the exception, just described, to the prohibition against doing what can be reasonably foreseen to cause loss of life (Scanlon 2008 p. 29).

Scanlon goes on to argue that both the intention and the action of TB are wrong. The intention of TB is wrong in the critical sense: it is a bad decision for which TB should be blamed. The act of TB is wrong, he argues, in the deliberative sense: not because of the

intentions of TB but because of the consequences of the action, namely the killing of non-combatants (Scanlon 2008 p. 29).

Scanlon states that TB is impermissible because the "death of non-combatants is not rendered a 'military advantage'". However, he does not present an argument to defend this. Why is it that the deaths of non-combatants should not count as "a military advantage by the fact that it would shorten the war by undermining public morale"? Shortening a war by whatever means strikes me as a very clear military advantage, and one which could minimize harm to non-combatants who might suffer more from a prolonged war.

As a result of his rephrasing of the principle of discrimination, Scanlon is unable to argue why it is that non-combatants should not be targeted by the terror bomber. If we take shortening a war to be a military advantage, and accept that the intentional killing (targeting) of non-combatants would shorten the war, then by Scanlon's argument the targeting of non-combatants would seem to be acceptable. The only way for him to avoid this conclusion would be to give the killing of a civilian an extremely high weighting. This would leave him in a position in which the killing of civilians is virtually forbidden.

A general prohibition against killing civilians might at first glance seem to be attractive and not too dissimilar from Vitoria's position presented above. However, there is an important difference between a prohibition against *killing* non-combatants (Scanlon) and a prohibition against *targeting* non-combatants (Vitoria), as I shall demonstrate.

I have argued that the act which is prohibited by the traditional principle of discrimination as presented by Vitoria is the *intentional* killing (successful targeting) of non-combatants. This accepts the unhappy truth that non-combatants are often killed in warfare without allowing for them to be targeted should it prove militarily advantageous to do so. By contrast, Scanlon's version of the principle looks as if it would prohibit the *killing* of non-combatants. This would render many forms of warfare illicit, such as bombings, missiles and sieges, even when those forms are commonly accepted. It is a sad but true state of affairs that non-combatants are killed in wars, be it from sieges, heavy artillery, or just happening to be in the wrong place at the wrong time.

The position that Scanlon advocates therefore falls to one side or the other of the traditional principle of discrimination as presented by Vitoria. It may be that Scanlon's position is more permissive of the killing of non-combatants in war. This would be the case if it could be shown that to kill the non-combatants would result in a military advantage. Alternatively it may be that Scanlon's position is less permissive, if the weighting of civilian lives were such that to kill them would be virtually prohibited. In either case Scanlon has a problem.

In the more permissive reading of his principle it would seem that, counter-intuitively, it is acceptable to kill large numbers of non-combatants if to do so presents a military advantage. This amounts not only to accepting the terror bomber's argument, but actually endorsing it. In the less permissive reading of Scanlon's principle many forms of contemporary warfare (e.g. missiles and aerial bombardment) and traditional warfare (e.g. artillery and sieges) would be impermissible. Again this is counter-intuitive. While the permissibility of many forms of contemporary weaponry (e.g. anti-personnel landmines, chemical weapons, biological weapons and nuclear weapons) has been discussed at length, the use of missiles and aerial bombardment *per se* has not formed a part of this debate. This, I would suggest, is because most people do not see anything fundamentally wrong with this form of weaponry. Indeed, if this less permissive reading of Scanlon's principle is correct then almost no war could be prosecuted justly in the age of missiles and aerial bombardment owing to the fact that the use of these weapons will likely result in the deaths of non-combatants.

Scanlon's rephrasing of the principle of discrimination such that the notion of intention is removed from the definition is hence unsuccessful. The conclusions to which it leads are counter-intuitive and would require a more robust defence than Scanlon provides. By contrast, the traditional principle of discrimination as presented by Vittoria focuses on the targeting, rather than the killing, of non-combatants.

Vitoria's approach holds several advantages over Scanlon's in that it offers more than mere proportionality. Rather it appeals to a principle of justice that non-combatants are such that they can never be targeted (killed intentionally), and defends that principle. On Vitoria's reading therefore, TB, which seeks the targeting (intentional killing) of non-combatants

must be wrong. By contrast SB, which does not target (intentionally kill) non-combatants, may be acceptable.

Vitoria's position sits more comfortably with the pre-theoretical response that many have upon reading SB and TB, namely that SB is morally permissible whereas TB is not. Scanlon is quite right to challenge this pre-theoretical intuition, in the sense of holding it up to the light in order to determine whether it can withstand a number of attacks. However, whereas Scanlon believes that he has demonstrated a lack of grounds for this intuition, I have argued that he has failed to demonstrate any such thing. Rather, I have suggested, the intuition is correct and in the absence of defeaters from Scanlon should remain in place.

Furthermore, I have argued that Vitoria's position sits more comfortably with common approaches to morality in war. In trying to reframe the principle of discrimination such that it carries no reference to intention Scanlon has produced a principle which is either too permissive or too restrictive. It either allows for mass killings of non-combatants for military advantage or it implies that virtually no war could be prosecuted justly. In either case, Scanlon's reworking of the principle is counter-intuitive and lacks persuasive force.

This discussion of the principle of discrimination may seem to have strayed some distance from the moral relevance of intention. However, it demonstrates how Scanlon has managed to overlook the fact that acts such as targeting are by definition intentional. Once the inherent nature of intention to the act is recognized it becomes clear that the act cannot be adequately described without the inclusion of intention. Contra Scanlon, the inclusion of intention in describing the act is therefore essential to understanding the permissibility of the act.

To draw this back to the discussion at the opening of this chapter concerning the distinction between Hero and Stalker, I claimed that the intention of the camera operator was morally significant in determining whether the act was permissible or not. I suggested that this may be related to differences in outcome that could result from the different intentions, but even if the outcome is the same in both cases I made appeal to a sense that Stalker was unjustified in his actions whereas Hero was not. Subsequently I have examined the arguments of Scanlon to consider his challenges to this intuition. In finding his challenges

unsuccessful, I suggest that the intuition remain unless and until a suitable defeater can be found.

5.4 Conclusion

I have argued that the consideration of intentions is a significant factor in the ethical assessment of surveillance. When the intention is the same as the just cause there is little concern about the intention *per se*. When, on the other hand, the intention differs from the just cause there is reason for us to sit up and take notice. I have described four reasons as to why it is important to consider intention as well as just cause. The first of these is what I have called the "soul of the perpetrator" and defined in both theological and non-theological terms; the second is the impact on outcomes of intentions in real world cases; the third is the problem of smokescreens; and the fourth the inherent value of intention.

I then considered objections to the consideration of intention as morally relevant put forward by Thomas Scanlon. Scanlon would not have a problem with seeing intention as morally relevant where it has an impact on effects. However he does challenge the inherent value of intention in determining the permissibility of an action where there is no impact on effects.

I critiqued Scanlon's challenge using two arguments. In the first, following McMahan, I argued that Scanlon confuses the scope of moral responsibility in both PMC and PRD. In the former case the prime minister is not responsible for the intentions of the bomber, and in the latter the patient (according to Scanlon) does not care about the intentions of the doctor. This is not that surprising, however, and contributes nothing to an understanding of the permissibility of the act. As McMahan has pointed out, each person is morally responsible for that over which they have control. The prime minister cannot control the commander's intentions any more than the patient can control the doctor's. Nonetheless this has no bearing on whether the commander or the doctor is right to carry out the action that they do.

I also argued that, despite the fact that the prime minister is not responsible for the commander's intentions, were he to discover that those intentions were in favour of killing non-combatants, he would be rightly shocked and would remove the commander from his

post. In this way, while the prime minister cannot control the commander's intentions, he can control which commanders to use. Likewise, should the patient discover that his doctor wanted to kill him rather than relieve his pain, he would again be unhappy with this and justifiably argue for the doctor to be struck off. Once more, the patient may not be able to control the doctor's intentions, but he may be able to control which doctor treats him.

Secondly, I argued that there are some acts which, in terms of assessing their moral permissibility, are inseparable from the intention underlying them. Targeting people is one such act which cannot be done "unintentionally" or "merely foreseeably". Scanlon misses this in the case of PMC by reframing the principle of discrimination such that it does not include reference to targeting or intentional killing. Instead he treats the bombing of non-combatants in war as wrong unless it can be shown to be proportionate to military objectives.

Scanlon's reframing of the principle of discrimination is, I argued, either too permissive or too restrictive. It would be too permissive in that it may be taken to allow for the mass killing of non-combatants, if those killings could be shown to be proportionate to military objectives. Alternatively it would be too restrictive if it were taken to give non-combatants a heavy weighting in comparison with combatants such that the former could never be killed. In this latter understanding almost no war could be prosecuted justly, especially in the age of bombs and missiles. Either reading of Scanlon's reframing of the principle of discrimination is problematic. What is wrong is therefore not the killing *per* se but the *intentional* killing (or targeting) of non-combatants. As such it is imperative that the intentions of the commander are known in order to determine whether the act is permissible or not.

Scanlon is thus unsuccessful in his attempt to deny the moral relevance of intention. Given the reasons I listed at the outset of this chapter, and in the absence of any defeaters by Scanlon, I believe that intention is relevant to the permissibility of actions. In conclusion, therefore, I believe that it is correct to include an assessment of an agent's intentions in assessing the permissibility of the actions carried out by that person for the reasons listed above. This is no less true in surveillance than in the other cases considered above. As such, any determination as to whether an act of surveillance is justified should take into account the intention underlying the reason for that surveillance taking place.

6. Authority

"How is your sex life?"

"Do you have a sexually transmitted infection?"

"How did you vote in the last national election?"

"What do you earn?"

If a stranger were to ask you any of these questions, the chances are that you would (respectfully) respond: "It is none of your business." This is a common phrase signifying that a question has probed too deeply into someone's private life. However, to say that something is none of your business suggests that it is perhaps of someone else's business. It might be no more than the respondent's business, such as voting, but it may also be that of a third party. My neighbour's income may be none of my business, but it is the business of the Inland Revenue. Whether you have a sexually transmitted infection is none of my business but could be the business of your physician, or of any sexual partners you have.

Whose business it is can be very specific. If my son is being bullied by another pupil at school this is not (necessarily) a matter for the police or social services. It is not even the business of "the school" (in the sense of all staff and pupils), nor of the teaching body (there are teachers who may never interact with my son or his persecutor), but of specific individuals in clearly-defined roles. It is a matter for the headteacher and my son's class teacher at school. In referring to such individuals we tend in everyday language to say that they have the "authority" to know. We describe them as being "in authority" over both my son and the bully.

The notion of authority, by which I mean morally legitimate authority, is also present in the examples of the Inland Revenue and the physician. In both cases we say that these bodies have the authority to know pertinent information about an individual. This seems broadly akin to the statement that knowing this information is "their business." Furthermore these authorities are sometimes justified in knowing this information with or without the subject's permission. It may be essential to the purpose of these authorities that they have access to particular information. If so, and if the organisation's existence is justified, then

so is the access that they have to this information. However, the means used to gain access may be unjustified.

For many the term "authority" has negative connotations. It can be seen to imply control and domination by the authority and a lack of autonomy on the part of the non-authority. Contemporary western culture, from Star Wars to the Social Network, frequently celebrates the rebel who challenges figures of authority. In the case of surveillance at least, though, I argue that authority is a good thing, that it is beneficial to society to have authorities. Authority is what distinguishes the police officer entering your home with a warrant from one without a warrant and, for all its potential flaws, I argue that that is an important distinction. If for whatever reason someone is going to watch me, I want that person to be someone who is appropriate for the role of surveillant. That is to say, that they have the authority to do so.

One reason that people may struggle with authority in the context of surveillance is that authorized surveillance can extend beyond that which is shared consensually (say, with a physician) to that which is not shared consensually (for instance, the police monitoring a suspected criminal). Authorized surveillance applies to both consenting and non-consenting surveillance. In the case of consenting surveillance authority is relatively uncontroversial: it is my business as surveillant because the surveilled subject has made it my business. In non-consenting surveillance, the claim that I have authority is the claim that someone's activities are (at least potentially) my business. This may be true irrespective of her wishes or even her knowledge.

Authorized non-consenting surveillance is not restricted to the state. If a headteacher has the authority to know about cases of bullying in her school, she is justified in knowing about these cases irrespective of the wishes of those involved (parents and children). She is also justified in mounting some level of surveillance in order to recover that information. Doing this places (or reinforces) her in a position of power and privilege over the surveilled subjects. I say "some level of surveillance" as there are questions of proportionality and discrimination which are relevant here. The head teacher is not automatically justified in reading the child's text messages nor in placing listening devices in the child's home in order to recover pertinent information.

The issue of authority alone does not solve the question as to whether surveillance is justified. Merely because I have the authority to monitor someone's activities does not mean that I should. Authority is one consideration to be taken into account among others. Furthermore, I shall argue that authority is not a necessary condition. It is plausible that surveillance could be justified in the absence of an authority. Nonetheless the presence of an authority offers *pro tanto* support in such justifications.

It is worth pursuing the question of permissibility. In the UK, the Border Agency (UKBA) has the legal authority to enter a person's property without a warrant. This does not mean that it is automatically permissible for them to do so, though. If the person in question were part of a paedophile organisation then it would be permissible for the UKBA to enter his property. If the subject were no more than an irritating neighbour of someone in the UKBA then it would not be permissible. Hence the notions of authority and permissibility are distinct, although related. A rule of thumb might follow that if I do not have the authority to act then what I do is not permissible unless demonstrated otherwise. This does not correlate to the rule that if I *have* authority then what I do within the limits of that authority *is* permissible unless demonstrated otherwise. Authority alone will not justify the permissibility of an act of surveillance.

The distinctness of authority and permissibility raises challenges when applied to surveillance. Take the case of private investigators (PIs). Is it permissible for John, a librarian, to sit outside Samantha's house and photograph her in her bedroom? Presumably not: this would make John a peeping Tom. Actions of this nature are intrusive and generally unacceptable. Yet if John were a policeman and had good cause for his actions (for example, good evidence that Samantha is dealing class A drugs in her bedroom) then it would be permissible. The case of PIs forms a grey area between John the librarian and John the policeman. If the John is a registered PI then he looks similar to John the policeman. If John is an unregistered PI then it is harder to distinguish between the PI and the peeping Tom. This makes John the PI look closer to John the librarian. It is hence important for John that he be registered. However, in countries such as the UK registration is not currently an option for PIs. I return to consider this issue at the end of this chapter.

There is a similar question of authority in the ethics of warfare. The just war tradition has, from its initial codification by Thomas Aquinas, included a requirement that war be

declared only by the correct authority (Aquinas 2000 pp. 1353–54). This is not to say that an authority may declare war at will: there are other conditions which must be met in addition to authority. Nonetheless, in the absence of authority justification would be harder. Furthermore, many today would dispute that one must have authority in order to prosecute a just war, as for example in uprisings against dictatorships. As in surveillance, authority in war is a *pro tanto* rather than a necessary condition. There is hence a similarity in referring to authority in both war and surveillance. Unless you have the appropriate authority, and in the absence of counter-arguments which I shall discuss below, it simply is not your business either to monitor my telecommunications or to declare war on me.

The issue of authority can therefore help to solve the question as to whether an act of surveillance is justified. If all other conditions (proportionality, discrimination, etc.) are met but the proposed surveillant is not an authority, then the ensuing surveillance would be harder to justify. If, on the other hand, all other conditions are met and the proposed surveillant does posses this authority, then the surveillance would be ethical.

As authority does not resolve permissibility and is not a necessary condition, it is unsurprising that it receives little attention in the literature on the ethics of surveillance. Graham Sewell and James Barker do not mention authority in their considerations of what renders surveillance ethical (Sewell & Barker 2001), and nor does John Kleinig in his nor David Lyon in his (Kleinig 2009; Lyon 2001). (Although in personal correspondence, Kleinig has stated that he was concerned with cases of surveillance by existing authorities.) Gary Marx comes the closest in raising authority as an issue, but only in a very specific manner (Marx 1998). Of his 29 "questions to help determine the ethics of surveillance", numbers 10, 12, 13, 14, 15 and 16 can be seen to refer to issues pertinent to authority as follows:

> 10 asks whether a tactical decision was arrived at through public discussion;
>
> 12 asks whether people are aware of the results of the surveillance;
>
> 13 asks whether there are procedures for challenging the results of surveillance;

> 14 asks whether there are appropriate means of redress for those who have been treated unfairly and means of accountability to encourage responsible surveillance behaviour;
>
> 15 asks whether the information can be protected adequately; and
>
> 16 asks whether there is favouritism in the availability and application of surveillance.

Each of these has a bearing on authority, but never once does Marx stipulate that there be an authority to legitimate the surveillance, nor is not clear whether these are necessary or merely desirable conditions.

The claim that authority can help to resolve the question of whether surveillance is ethical raises a number of questions about the nature of authority in the case of surveillance. These questions will be dealt with in the three major parts of this chapter. Firstly, I ask what authority *is*. My position here is that an authority insofar as it relates to surveillance is a trusted and accountable person, occupying a role for which surveillance is necessary but limited by context, on whom authority has been conferred by a suitable entity. This is a dense definition and I take the majority of the chapter to develop it. Secondly, should there even be a concern about authority? Given that others have neglected to refer to it, perhaps it lacks moral relevance. I argue conversely that it is a morally relevant consideration and that to ignore it is an oversight. The third question asks whether authority is a necessary condition for surveillance. Here I argue that it is not a necessary condition as there are situations in which a surveillant who is not an authority may be permissible in carrying out surveillance. However, such situations are the exception rather than the norm. Finally I support the claims made in this chapter by considering three examples of authority in surveillance, demonstrating the difference that is brought to each case by the consideration of authority.

Throughout the chapter I make the core assumption that, unless stated otherwise, all other conditions for justified surveillance are met. That is, there is a justified cause, the intention is correct, surveillance is a proportionate response, it is necessary and it stands a chance of success, and that the method of surveillance is both discriminating and proportionate. I

shall draw primarily from the just war tradition in the discussion. As noted, authority was one of the conditions of a justified war as codified by Aquinas and remains so nearly a thousand years later. In the following discussion I will demonstrate the value of drawing upon that tradition to answer the question of authority in cases of surveillance.

6.1 Defining Authority

6.1.1 Authority as Trusted

What is authority within the context of surveillance? In monitoring a person, the surveillant is placed in a position of privilege and power vis-à-vis the surveilled subject. This position carries with it a degree of responsibility, owing to the harm that can be visited on the surveilled subject. There is more to authority than the mere avoidance of harm, though. When a person has authority this carries with it an implication that someone trusts that person to make good decisions in the area of his authority. For someone to be placed in a position of authority they will typically have demonstrated the capacity for good decision making in the past. An authority in surveillance is therefore someone who is trusted by another to make good and responsible decisions as to whether and how to use surveillance. The information on which decisions are based may be limited. The authority is then trusted to make good decisions with the information available. Sometimes that information will only be available to the authority, and so the level of trust is greater. In declaring war an authority may act on information which is unavailable to the public. In such cases the public places great trust in the authority that they have good reasons for their actions. Similarly in surveillance, authorities are trusted to have good reasons for their actions.

It would be strange for a person to be given authority to mount surveillance merely because he were trusted, though. I trust my best friend but that does not give him the authority to mount surveillance on suspected criminals. My trusting him may make it more likely for him to become an authority, but there are other relevant factors than mere trust. His training, interests, capacities and availability would need to be taken into consideration. It is more natural that if a person is *not* trusted then this excludes him from occupying a position of authority. Merely being trusted is insufficient to qualify a person as an authority to carry out surveillance.

I have referred to a *position* of authority. If the person *qua* individual lacks the authority for surveillance, what of the role that person occupies? This makes more sense. Authority appears to be intimately linked to role. An employer has the authority to monitor employees, the state has the authority to monitor criminals, headteachers have the authority to monitor pupils while at school, and parents the authority to monitor their children (until those children reach the age of majority). However, it is strange to speak of trusting a role. I do not trust the *position* of headteacher, nor do I trust the *role* of employer. Indeed, I know how readily such positions can be abused. Instead I trust the person occupying that role. In occupying a role the person is either assuming the authority as a matter of natural course (i.e. as parent) or they have had that authority conferred upon them. If the latter then the person chosen for the role should be one, as noted above, who is trusted in that role. If trust is lost then the person should lose the authority associated with that role and so relinquish the position. If he does not relinquish the position then a situation arises in which he *should* have authority to function in the role but does not actually *have* authority, because he has demonstrated that he cannot be trusted.

Authority does not reside either in a person or in a role, therefore, but in the person occupying a role. Hypothetically, let us say that Jane is always trusted and Jane is a headteacher, so Jane is a trusted headteacher. As such I am happy to recognise the authority of Jane-as-headteacher to monitor my children while in the care of her school. Jane would not have this authority if she were to pass by another school and stop to monitor the children in that school. This would be true if she were motivated by the same virtuous reasons as would motivate her carrying out surveillance in her own school. Similarly, even in her role as headteacher she would not have this authority in her own school if she demonstrated that she could not be trusted to make good and responsible decisions regarding surveillance. Hence it is neither Jane nor the headteacher who has authority, but Jane-as-headteacher.

6.1.2 Authority as Accountable

Authority implies a person is trusted to make good decisions based on the information available. The identification of a "good decision", though, is not restricted to that authority. The criteria for a "good decision" may be discussed and agreed publicly. This is the case regarding war in the democratic tradition, where the reasons for declaring war are publicly

discussed before, during and after wars. The same is true of surveillance. Acts of surveillance, when they come to light, may be discussed in the public square and conclusions reached as to whether they were justified. The authority is hence held accountable to the public. This serves to limit abuses by the authority. Accountability requires that a higher authority (often the public or a person acting on behalf of the public) is able to strip the surveillant of their authority should such abuses emerge. This may be achievable directly through voting the person out of office, or indirectly by placing pressure on a proxy to remove the person from office.

This accountability is illustrated in a recent case of war. In 2003 the claim was made by authorities in the UK and US that Iraq was developing weapons of mass destruction which could be used against those countries. This claim was based on intelligence which, it was argued, could not be released to the public for reasons of national security. If this intelligence existed and were accurate then many felt that it could be used to justify the declaration of war. However, the reliability of the intelligence was a matter of trust that the publics of the UK and US had to place in their respective authorities. That trust was damaged when it later transpired that the intelligence was not reliable (Drogin 2008). The authorities in the UK and US did not lose their authority to declare war (they did not lose all of the public's trust), but they did diminish it (they did lose some of the public's trust). Future claims justifying military action would have received greater scrutiny than before. Were it to be revealed that they had known in advance that the intelligence was unreliable or even false, then they could have lost all of the public's trust. In that case the individuals would have forfeited their legitimate authority and should have been removed from their positions.

Once again authority exercised in surveillance is similar. A headteacher has the authority to monitor pupils in her school. She holds this authority as she has demonstrated the capacity to make good decisions regarding such surveillance. One hopes that if she had made consistently bad decisions this would count against her becoming a headteacher. The implication of the authority she possesses is that she will be trusted with information which is not available to everyone, in order to make good decisions. Should it transpire that she has placed CCTV in the school locker rooms not to combat drug-taking but rather for prurient reasons then this trust would be diminished and she should forfeit her authority.

In both the state declaring war and the headteacher employing surveillance, trust is placed in the relevant authority that they are likely to make good decisions. Should evidence emerge of their having made poor decisions then this might shake the trust sufficiently for them to be forced to relinquish their position.

Authority therefore involves trust in and accountability of a person occupying a role. If the person is not trusted then he does not have the authority that is normally associated with occupying that position. If successive individuals lose the authority associated with a particular position then it may be that the position ceases to be a relevant consideration in relation to authority. If every police chief in a twenty-year period were corrupt then the problem could lie with both the individuals *and* the position they occupy. Indeed, it may transpire that the position is such that one cannot occupy it without being or becoming corrupt.

6.1.3 Authority Limited by Context

There are further limitations on authority beyond those placed by trust and accountability. For instance, my trusted and accountable employer does not have the moral legitimacy to watch me at any time. Rather my employer has the authority to monitor at least some of my behaviour whilst I am actively engaged as his or her employee in the workplace. When I leave the workplace, or my context of work, my employer's authority ceases to have effect. This might alternatively be phrased such that my employer has the authority to act as my surveillant (with certain restrictions stemming from just cause, proportionality, etc.) only within the context of my workplace. This should come as no surprise. My employer likewise has the authority to discipline me for actions which I perform as an employee in the context of my work, but not for actions outside of that context. I may for instance be dismissed for inappropriate behaviour at work, but not for inappropriate behaviour at home or at a pub (unless my activity in *that* context has some bearing on my ability to perform my work).

As with the employer so with the headteacher. The head teacher has the authority to carry out surveillance within the context of her school. However, she does not have the authority to carry out the same in the context of a different school or a non-school context. Her authority is restricted to the context in which it is relevant. It will be seen on reflection that

this is true in all other cases of authority as well. The scope of authority is always limited by the context in which the authority operates. Hence the authority of a sovereign extends only over the denizens of that sovereign's state; of parents over their own children; and of carers over those in their care.

6.1.4 Authority as Conferred

I have stated that a person in authority should be trusted and held accountable, and occupy a role and be in a context for which surveillance is appropriate. However, that person must come to be in that role in some way. That is, he must gain his authority.

There are two ways in which we describe a person as coming to have authority over another. Either that authority is natural (it is, in some way, in the natural order of things) or it is conferred by another person or people. In saying that authority is natural I am not referring to people who are described as having "natural authority". This is the description of a character trait rather than a moral status. Rather I am referring to scenarios involving the family such as the roles of parent and child, or possibly the oversight of a family member who has severe mental health problems. There is something in these roles that suggests that this authority is in the way of "how things should be", that humans are in some respect predisposed to act in this manner. I am using "natural" here in a manner similar to how it is used in "natural rights" as opposed to "legal rights".

The second means by which we typically describe a person gaining authority is when it is conferred. Authority can be conferred from above, horizontally, or from below. It may be conferred from above if granted by a superior, horizontally if granted by peers or from below by those expressing a desire for such authority over them. In the UK the prime minister is installed by the head of state (from above), chosen as a candidate as head of the party by his or her peers (horizontally), and chosen as a member of parliament by the electorate (from below). In each case there is a requirement that those granting the authority have themselves the authority to grant it. In many countries only the head of state, rather than perhaps the armed forces, can constitutionally grant a person the authority to be prime minister. The decision to make a person head of a political party is made only by those in that party (fellow members of parliament and/or party members). Finally, in electing officials to office the election can only be participated in by those who are citizens

and of a legal age to vote. Unlike the situation between parents and children there is no "natural authority". Such a natural authority was once claimed by those who believed in the divine right of kings, but is generally no longer adhered to in democratic states. Rather the people confer authority onto another individual as and when it is deemed necessary, for instance when choosing a person to lead the government.

It is worth clarifying here that natural authority and conferred authority are not mutually exclusive. It is possible for a person to have both natural and conferred authority, as when a prime minister is also a parent. It is also feasible for a person to have just natural (a parent with no additional responsibilities) or just conferred authority (a prime minister with no family responsibilities). Finally it is of course possible to have no authority, natural or conferred.

It is important to note that I am here describing how people *gain* authority. A person may gain authority in a natural sense, but still be held accountable to the public. Neglectful or abusive parents may have their authority as parents revoked by society (as in the case of Peter Connelly, more popularly known as Baby P (Sellgren 2010; Batty 2009)). They lose their authority through an abuse of the position they occupy. In some countries people deemed unsuitable to be parents (e.g. paedophiles) may be prevented from having children through forced sterilization (Baczynska 2009). In such cases these people are prevented from gaining authority over children by society. Nonetheless it would seem forced to say that for the most part parents had their authority over their children conferred upon them by society. There is no social decision-making process by which it is decided who can be parents.[8] The closest in which we come to this as a society is in reviewing the suitability of parents to adopt children. However, in this case the children have first been entrusted to the state and so it is reasonable that the state ensures it can trust the prospective parents of these children.

The possibility of losing one's natural authority as a result of abuse opens an asymmetry in gaining and losing authority. One may gain authority as a result of nature, without societal

[8] Idealistic communist visions have been presented of children being raised by the community (for example in Plato's *Republic* or Huxley's *Brave New World* (Huxley 2007; Plato 2007)) but I am not aware of any historical case where this has happened, although there are cases in which a person may be *prevented* by society from becoming a parent, or from keeping their children, as demonstrated above.

involvement, but then lose that authority as a result of abuse coupled with society's strong disapproval. This asymmetry does not exist in the case of conferred authority. Here a person is given authority because he is trusted by another with the authority to confer, and then loses that authority when he is no longer trusted by that conferring authority. The conferring authority will himself be subject to criteria of trust and accountability, ensuring that authority should not be revoked arbitrarily but only on the grounds of reasonably diminished trust.

The process of conferral allows for inconsistencies to arise in how we use and reflect upon authority. A person may be conferred with authority from above by a patron, such as a prime minister awarding positions in his or her cabinet. However, the new minister may have gained this position through family connections or blackmail, rather than fulfilling the requirement of being trusted. In this case the minister occupies a position of authority without being an appropriate person. Given the definition worked out so far, this person does not have moral authority.

The case of an inappropriate person being given a position of authority introduces an important distinction between moral authority and (mere) titular authority. Mere titular authority is the result of conferral alone, with no accompanying moral authority. A person with titular authority therefore may or may not have moral authority as well. Alternatively, a person may have moral authority but no titular authority. Then again, a person may have authority conferred on them and be trustworthy. Trustworthiness, as opposed to trustedness, is a character trait and does not reflect on how a person is perceived. Keith may be trustworthy but not be trusted. Luke may be trusted but not trustworthy. There are therefore four distinctions to be drawn in the case of conferral:

1. Mere titular authority (conferral without moral authority)
2. Conferred authority based on character (conferral with moral authority based on trustworthiness)
3. Conferred authority based on experience (conferral with moral authority based on trustedness)
4. Mere moral authority (moral authority with no conferral)

Mere titular authority is problematic, as outlined above, because it allows for a person to gain a position of authority without having the appropriate moral authority. This would be insufficient in seeking a justification for actions such as surveillance. Given that a person's moral status is unknown in the case of mere titular authority, it has little to offer regarding justification.

This leaves three alternatives: authority based on character, authority based on experience, and mere moral authority. From a moral perspective it would seem preferable to have a person in authority who has the better character. However, a position of authority involves having authority over people. If the person in authority is trustworthy but not in fact trusted then he or she will likely have no *effective* authority. That is, the people over whom she wields authority would not trust her and so refuse to acknowledge her authority. This would be a problem for the exercise of that authority.

The third alternative is for authority to be based on experience. I have argued that the relevant experience in the case of surveillance is trust. Trustedness overcomes the pragmatic concern associated with trustworthiness, but it is subject to popular fickleness. A person may cease to be trusted, for example, on the basis of an incorrect newspaper article which slanders his reputation. It is also strange to prefer the less morally upright person (i.e. one who is trusted but not trustworthy) who may be good at reputation management over one who is less media-savvy but a genuinely more trustworthy individual.

One way around this difficulty is to insist upon accountability. A person in authority must be trusted to be effective, but to be trusted they should be trustworthy. Over the long term few would continue to trust a person who has demonstrated themselves to be untrustworthy. As a conferred position over another, then, a person in authority must be trusted if that authority is to be effective. However, by ensuring that the person is accountable then his character will be revealed over time. Through an authority's decisions being held to account, it will become clear whether or not he is trustworthy. If he is trustworthy then he will continue to be trusted. If accountability reveals him to be untrustworthy then he will cease to be trusted. Accountability therefore serves to bring together the character of a person (trustworthiness) and the experience others have of that person (trustedness).

The fourth alternative is mere moral authority. This is also problematic, although for different reasons. If authority is not based on a natural relationship, nor is it conferred, then it rests solely on the person's claim to moral authority. This does not carry the same weight as conferred authority. However, there are mitigating circumstances, such as the total absence or corruption of any conferring authority, in which mere moral authority is sufficient to temporarily occupy a position of authority. I shall consider this scenario in further depth below.

Hence an appropriate person to be conferred with authority is one who is both trusted and accountable. This discussion reinforces the importance of trust and accountability while at the same time demonstrating the need for conferral of authority and clarifying the distinction between titular and moral authority. The definition of an authority can now be extended to: a trusted and accountable person, occupying a role and limited by context, on whom authority has been conferred by a suitable entity.

6.1.5 Authority of Roles

I have considered a number of cases so far which range from the context of the family, to that of the workplace, to criminal activity. In each context there may be a different entity with the authority to mount surveillance. Hence the authority to monitor children belongs in the first instance to the children's parents or those acting in *loco parentis* such as a school, nanny or babysitter. Should the parents fail in this responsibility and thus demonstrate negligence, then and (only then) the authority to monitor the children passes over to the community or state. Similarly the authority to monitor employees, through for instance insisting on the stamping of timecards, belongs to the employer in the context of the workplace. Out of the workplace the employer does not have this authority, and even within the workplace such authorized surveillance is not total owing to further considerations such as proportionality and discrimination (i.e. it should not ordinarily extend to toilets in the workplace). Within the workplace the state has no standard authority to monitor employees *qua* employees, but only insofar as they may be suspected of criminal behaviour.

It is therefore possible to gain and suspend the authority to mount surveillance. I have argued that one may lose authority by demonstrating that they cannot be trusted to make

good and responsible decisions. I have also suggested that one's authority is limited by context. When the surveillant or the subject under surveillance leaves that context the authority is suspended. Thirdly I have claimed that a person gains authority through the process of conferral. It remains to be seen which people should be conferred with authority. So far these arguments revolve around the person. However, I have argued that authority concerns a person *occupying a role*. It therefore remains to focus on which roles should be conferred with the authority to carry out surveillance.

To resolve which roles should be conferred with the authority to carry out surveillance one can refer to what is appropriate in a particular context. It is appropriate for a headteacher to have the authority to carry out surveillance in the context of her school, but not of another's school nor of a pupil's home. It is appropriate for the police to have the authority to carry out surveillance in the context of a person who is reasonably suspected of committing a crime, but not of a person for whom there is no evidence of wrongdoing. It is appropriate for a physician to know about my medical history, but not (necessarily) appropriate for my employer to know the same. It is appropriate for the police to know of my criminal record, but not the supermarket where I hold a loyalty card. In some contexts, such as the medical or work arena, what is appropriate is generally well-established and recognized. In other areas, such as social networks on the internet, what is appropriate to share is more controversial (Nissenbaum 2004; Rachels 1975).

Appropriateness alone, though, does not go far enough in clarifying which roles should be conferred with the authority to carry out surveillance. How is it that we deem some roles to be appropriate and others not? In some ways this just pushes the question back one step. It may be helpful in terms of establishing social norms, but not ethical imperatives. Granted we see the physician as an appropriate role to know my medical history, but it does not follow that the physician *should* be an appropriate role to know my medical history.

The principle underlying appropriateness in each of the above cases is necessity in order to perform the role. The role could not be adequately carried out if the holder of that position did not have access to surveillance. Hence bullies, knowing they will be punished if caught, typically carry out their bullying away from teachers. The headteacher could not be sure to know of cases of bullying in her school if she were not to carry out some level of

surveillance of the pupils.[9] Likewise criminals generally hide their criminal activities. While the police will be aware of the activities through complaints by the victims, to discover the culprits they often need to use surveillance. Were surveillance not available to them as a tool then they might never discover the identity of the criminals behind the acts.

In contrast to these cases, let us assume that my work is such that it is not necessary for my employer to be aware of my medical history. That is information which could become available to him through surveillance, but it is not necessary for him to know it in his role of employer. It might also be detrimental to me were he to discover my medical history. Such knowledge could unfairly prejudice him against me if, for example, it revealed my homosexuality and he were homophobic. It is therefore appropriate that he not have this information: it is not necessary for him in his role of employer, and it is important for the security of my employment that he does not have access to this information.

A further problem is that some roles require surveillance in order that they be carried out properly, but the roles themselves are unethical. Imagine the pimp who needs to monitor the sex workers he "manages" both to offer them protection and to ensure that he collects his share of their income. It could be argued that the surveillance is necessary for a pimp. However, pimping is an unethical activity. It would be wrong to say that the pimp has the moral authority to carry out surveillance because it is necessary to his role. Developing criteria for ethical roles goes beyond the scope of this chapter. Instead I shall state a simple proviso that if the role is not ethical then holders of that position cannot claim authority for surveillance purposes.

The central question in addressing which roles should have the authority to carry out surveillance is therefore the necessity of a person occupying that role having access to surveillance in order to carry out the role properly. If on the other hand the role can be performed properly without surveillance then it would be inappropriate for that role to carry with it the authority to carry out surveillance. Finally the role must not be unethical in order to qualify the role holder for a position of authority.

---

[9] Note that I am not necessarily advocating technological surveillance. The eyes and ears of the head teacher and other members of staff are a type of surveillance.

6.1.6 Conclusion

I have argued that an authority should be a trusted and accountable person, occupying a role for which surveillance is necessary but limited by context, on whom authority has been conferred by a suitable entity. This definition provides sufficient and necessary conditions for determining whether a person has the authority to employ methods of surveillance. As a short-hand, the definition could be said to stipulate that an authority is an appropriate person in an appropriate role operating within an appropriate context. The longer definition serves to clarify what is meant by each use of the term "appropriate." With this in mind I shall use "appropriate" from here on to refer back to the relevant part of the definition. With the definition complete I am now in a position to explain the value of having an authority in the context of surveillance.

6.2 The Purpose of Authority

I have mentioned Aquinas' inclusion of a principle of authority as important in justly declaring war. For Aquinas, this principle ensures a clear distinction between the private individual and the sovereign (Aquinas 2000 pp. 1353–54). While the private individual could seek redress of wrongs through the courts, there were in the thirteenth century no international courts to which a sovereign could appeal. As there was no higher human authority, the sovereign had the right to use coercion in maintaining the peace. This maintenance of the peace was true of both internal and external threat. It was because of this that it was the business of the sovereign to raise an army when necessary. According to Aquinas, though, it was always wrong for a (non-sovereign) individual to do this.

The value of authority in this context, according to Aquinas, is hence that it distinguishes between appropriate and inappropriate users of force. It is inappropriate for a (non-sovereign) individual to use force or to raise an army to redress a wrong as he can appeal to a higher authority. By contrast it is appropriate for the sovereign to use force and raise an army to protect its denizens from both internal and external attack. Of course a sovereign can still use force inappropriately by ignoring other aspects such as just cause or proportionality. However, the use of force or raising of an army by a non-sovereign individual will always be inappropriate if he does this to redress a claim within a just state

After Aquinas there is little discussion within the just war tradition as to why there is a need for authority, although there is some debate regarding the necessity of the authority condition. Contemporary writers in the tradition such as James Turner Johnson and Anthony Coady concur with Aquinas that the importance of authority lies in its ability to distinguish between legitimate public wars and illegitimate private wars such as feuding and brigandage (Coady 2007; J.T. Johnson 2007). As Coady writes, "the condition of legitimate authority has its rationale in the concern that the license to resort to war be restricted to political agents who might be expected to exercise more responsibility than private agents or criminal groups" (Coady 2007 p. 98). Such private agents or criminal groups may include the Italian Mafia, Chechen warlords, or right-wing privatised militias in the American heartlands.

The importance of authority in the just war tradition therefore derives from its ability to distinguish between the (inappropriate) use of force by private entities and the (appropriate) use of force by the sovereign. Private individuals or entities will always raise armies inappropriately if this is to redress a claim within a just state. The sovereign of the just state, however, is expected to demonstrate a greater sense of responsibility than the individuals within that state.

The discussion so far focuses on actions within a just state. What of an unjust state in which an individual seeks redress, but has no access to the courts? This does not appear to have been considered by Aquinas. Raising armies under these circumstances typically leads to terrorism and/or civil wars. If the authority principle is insisted upon within the just war discourse then this would render otherwise justified rebellion against an authority as illegitimate. This is the position taken by some commentators such as Anthony Coates (in Coady 2007, p.172) in arguing against the legitimacy of terrorism. However, this is inconsistent with the underlying principle of the separation of appropriate from inappropriate users of force. It is possible that an authority figure be so corrupt that the only way to remove him is by force of arms. In such cases the appropriate user of force would be the rebels rather than the authority.

The case of justified rebellion is interesting in light of the foregoing definition of authority. An authority figure which is sufficiently corrupt to spark a rebellion would surely have lost the trust of the people. If so then that figure no longer holds a position of moral authority

but mere titular authority. By contrast the leader of the rebels may have had authority conferred on him by the people, which some would consider a higher authority, and so qualify as trusted, accountable, context-limited and conferred. That is, the leader of the rebels may have a better claim to authority than the merely titular authority figure. If instead the leader of the rebels has not had his authority conferred then a vacuum in authority arises: one leader has mere titular authority while the other has mere moral authority.

I have argued that the justification for including the principle of authority in the just war tradition is to distinguish between appropriate and inappropriate users of force. This, though, relates to authority as it pertains to statecraft in general and warfare in particular. What value does this have in the underlying attempt to determine authority in surveillance? After all, the legitimate authority in war today is typically taken to be either the sovereign of a state or the United Nations Security Council. In terms of surveillance it would seem bizarre to limit the practice to a national or trans-national body.

Nonetheless, there does appear to be something *prima facie* wrong with just anybody being able to carry out surveillance on anybody else, just as there is something *prima facie* wrong with just anybody being able to raise an army and declare war. Furthermore, there is a distinction as noted earlier between a policeman listening to my conversations with a warrant and one so listening without a warrant. There are then appropriate and inappropriate users of surveillance, just as there are appropriate and inappropriate users of force.

This is not a point which needs belabouring. As referenced above, private investigators may operate in some states, such as the UK, without a licence. In such cases it is difficult for a surveilled subject unfamiliar with the industry to distinguish between a private investigator who is appropriate and one who is not. The value of licensing is that it clarifies this distinction through openly conferring authority on certain individuals and thereby recognizing them (rather than have them self-define) as appropriate users of surveillance.

There are some important disanalogies with the war scenario, though. The authority to decide to go to war rests, as noted, with a single body. This is traditionally the sovereign, but increasingly seen as an international entity such as the United Nations Security Council.

By contrast the authority to decide to use surveillance ranges across a number of contexts from the family to schools to the workplace to international espionage. Rather than seeking a single authority for surveillance as there is for war it is preferable to look for different answers responding to different cases.

Secondly, I have suggested that authority is not a necessary condition for justified surveillance. It is possible that a surveillant be justified without holding a position of authority. Although I have yet to defend this position, if I am correct then this bypasses the aforementioned dispute regarding justified rebellions. Surveillance is not restricted to conferred authorities but may justifiably be used by what I have called mere moral authorities. In this way popular surveillance of an authority may be justified if that authority has lost the trust of the populace.

6.3 The Necessity of Authority

I have argued that it is permissible for authorities to mount surveillance within limited contexts (headteachers in schools, employers in the workplace, etc.). If so then it is important to consider whether there are universal contexts in which just any person (*vice* a conferred person occupying a role) is an authority or is at least permissible in carrying out surveillance. If there are then this will challenge the importance of authority as a condition for surveillance. For example, in chapter 4 I argued that surveillance in the case of self-defence was a legitimate cause. Anyone may be the victim of life-threatening aggression and hence need to resort to surveillance as a means of self-defence, a scenario I shall refer to as Self-defence. There are other pertinent examples to consider, though.

Imagine that Alison has some dealings with her bank, causing her to go into the bank and stand in line waiting to be served. While Alison is in line a number of people enter the bank wearing balaclavas, intent on robbing the bank. Having disabled the CCTV system in the bank and taken away customers' camera phones they take off their balaclavas. This enables Alison to take a long, studied look at each of the robbers with the intention of describing their appearance to the police at a later time. I shall call this case Chance. Does Alison in this case need to be an authority to so monitor the robbers, or can she legitimately do this despite not being an authority?

Next consider Paternalism, in which Bill has taken his children to a local play park. Given that Bill has two children and that there are various opaque objects in the park (slides, etc.) he cannot watch both of them all the time. Imagine that Bill is distracted by watching one child on a climbing frame. Unbeknownst to Bill, his other child walks too close to a moving swing and looks as if he will get kicked in the head. I presume that Bill would not have a problem should another parent foresee this and keep an eye on the child so as to intervene if necessary to prevent harm. In the cases of Chance and Paternalism, do such eyewitnesses and "other parents" have the authority to monitor other people by virtue of being present, by being parents, by being citizens of the same community, or simply by being human?

In all three cases (Self-defence, Chance and Paternalism) I believe the surveillant would be permissible in carrying out the surveillance. The question here is whether the surveillance would be permissible because the surveillant is an authority or despite the surveillant not being an authority. If the latter then it cannot be the case that authority is a necessary condition for the permissibility of surveillance.

I take Self-defence to be a paradigm case of one person acting permissibly in carrying out surveillance on another. However, there is no sense of conferral of authority in this case, nor need the person be trusted to be justified in carrying out surveillance. Neither of these factor into the surveillant's basic right to self-defence.

The second case, Chance, differs from Self-defence in that Alison is not, I shall assume, personally threatened by the bank robbers. Irrespective of this difference, it would be strange to say that Alison is an authority insofar as surveillance is concerned. As a chance participant in the action, she is not necessarily trusted, she does not necessarily have a role appropriate to surveillance (she is not, for instance, a security guard at the bank) and nor has she been conferred in a role appropriate to surveillance. Nonetheless I think that Alison would be acting permissibly in recording and reporting the features of the criminals. Indeed, given that she might put herself at risk through acting in this way, many would applaud Alison's courage in becoming a surveillant. Nonetheless, Alison's role as a user of the bank does not necessitate her use of surveillance, nor has she had the authority to mount surveillance in this context conferred upon her by a suitable entity. Hence despite the permissibility of Alison's actions it would be wrong to consider her an authority.

The case of Paternalism differs again. There is a relationship of implicit or at least implied trust between Bill and other adults at the park that they all share in a common goal (allowing children to have fun) and share common interests (the protection and safety of their children). In this case the surveillant may be unknown and hence not trusted as an individual. However, in that person's role as parent or carer leading to her being at the park, Bill might assume a level of trustworthiness and hence choose to place his trust in the surveillant. It might also be assumed by Bill that, as parent or carer, the surveillant has had authority conferred on him by nature or an appropriate entity (the parents or the state), and the context is limited to that of a person acting in *loco parentis*. If so then Bill may assume that the surveillant is an authority. However, he may be incorrect in this. The surveillant may have kidnapped the children years ago and raised them as her own. As such the surveillant would not be an authority as there would be no accountability and the role of kidnapper is not ethical. It is also worth asking what would be the case of an adult passer-by who pauses to enjoy watching the children in the park and then looks out of concern at one walking too close to the swings. In such a case the passer-by would appear to be acting permissibly but without the stipulations which would classify her as an authority. In this case it appears once again as if a surveillant may be acting permissibly without being an authority.

There are therefore conceivable cases in which a surveillant acts permissibly despite not being an authority. In Self-defence and Chance the legitimate surveillant is not an authority, but rather any person who finds themselves in this predicament. In Paternalism authority may be assumed (perhaps wrongly), but in the passer-by variant there is again no authority. This demonstrates that a legitimate surveillant does not always need to be an authority, and thus also that authority is not a necessary condition for permissible surveillance. However, as noted above, authority does carry some moral weight in that it is helpful in distinguishing between appropriate and inappropriate users of surveillance. It is therefore a *pro tanto* as opposed to a necessary condition for surveillance.

Given that authority is a *pro tanto* condition I can return to the earlier claim that a rule of thumb exists such that a person who is not an authority is not justified in carrying out surveillance unless demonstrated otherwise. This brings together the intuition that not just anyone would be appropriate in carrying out surveillance and the possibility that a non-

authority surveillant could be justified. There is hence a reasonable assumption that a non-authority would not be an appropriate user of surveillance for a number of reasons (he may be unaccountable, untrusted, operating out of a pertinent context, or lack conferral). However, there are circumstances under which such a non-authority figure would nonetheless act permissibly in carrying out surveillance.

In the final part of this chapter I explore just how useful authority can be. To do this I will consider three cases: the surveillance of children, the licensing of private investigators, and the role of investigative journalists.

6.4 Authority Applied

6.4.1 Authority and the Surveillance of Children

To illustrate the value of these considerations I shall start by drawing on one of the least controversial examples of surveillant and surveilled subject: parent and (that parent's) infant child. It is unquestionably appropriate that someone monitors the child. Infant children require near-constant vigilance. Given this, it is right that the person watching the child should be an authority. I have argued that the value of an authority in this context is to distinguish appropriate from inappropriate users of surveillance, a part of which involves protecting the innocent from harm. Children are paradigm cases of innocence and vulnerable to injury. Insufficiently attentive surveillants could allow harm to come to the child, and abusive surveillance could cause direct harm to them. So infants require surveillance. That surveillant should be an authority, but there may be extenuating circumstances which would justify the surveillance of a non-authority figure.

According to the aforementioned considerations, the authority monitoring a child should be a person occupying a role who is trusted and held accountable, operating within a context-defined scope, and who has had the role of authority conferred upon him by a suitable entity. Applying this to the context of infant children, this means that the child's surveillant should be a trusted and accountable person who fills a role for which surveillance is considered necessary for the proper execution of that role. In this case the role could be parent or carer. Furthermore the person should pay attention to the child while the child is in his care (context). For both parents and carers this will be at all times when the child is

not with another parent or carer. Finally the role should be conferred in the case of a carer or may be claimed as natural by a parent.

All of these considerations help to reduce the likelihood that the child will come to harm. The surveillant is trusted to make good and responsible decisions in the context of childcare; he or she is accountable if these decisions are not made and carried through; he or she also faces the removal from authority if abuse of the position is discovered. In the case of carers, the parent or legal guardian should have conferred authority on the carer, ensuring to the parent's (or legal guardian's) satisfaction that the carer is suitable.

While uncontroversial, the case of overseeing children is obscured somewhat in that all adults have a duty to "keep an eye on" infants. It is not the case that a person who is not a parent or carer is therefore inappropriate to watch out for a child. A person with no children notices a child playing near the edge of a pavement next to a busy street, and whose mother is deep in conversation, would be entirely justified in keeping and eye on the child, ready to intervene in case he or she moves off the pavement and into the road. Secondly, infants do not have the same privacy interests as adults, so it would take something as extreme as posting inappropriate pictures on the internet to harm the child through surveillance alone. Infants are thus less at risk to harms from surveillance, and more at risk to harms arising from a lack of surveillance, than most adults. This has a clear affect on considering the justification of surveillance in the case of infants. The fact remains, though, that it is clearly preferable for an authority as described to be responsible for that surveillance.

6.4.2 The Private Investigator as an Authority

For a second case I return to the case raised earlier regarding private investigators (PIs). For the purposes of this discussion I shall assume that PIs fulfil an ethically justified function in society.[10] A major part of any PI's work is surveillance, either directly through tailing and recording a person or indirectly through examining databases. Without this surveillance it is questionable as to whether most PIs could continue to operate. Surveillance is therefore a necessary part of their work.

[10] The broader ethics concerning the justifiable existence of private investigators are an issue for a separate discussion.

There are clearly appropriate and inappropriate people to fulfil the role of surveillant. Inappropriate people are those who are not trusted, who are unaccountable for their actions, who have abused the position of surveillant in the past or are doing so at present, or who operate outside the context of their particular case. In such cases there is little to distinguish the PI from a stalker.

By contrast, appropriate PIs are trusted and accountable, do not abuse their position and restrict their surveillance to their particular caseload. To all intents and purposes they are surveillance authorities. The one thing that sometimes prevents them from becoming an authority is the absence of a licence. That is, they have not had their authority conferred.

In the absence of conferral of authority, the public is left in the dark regarding whether a particular PI is appropriate. People might look for recommendations, but these may not be reliable or forthcoming if others do not wish to advertise their having used a PI. Without conferral the public is unable in the first instance to distinguish between a legitimate and an illegitimate authority in terms of PI surveillance.

There is a dangerous alternative in which the PI may hold just a licence and not actually be an appropriate user. In this case, as discussed earlier, the PI would hold mere titular authority, which may be worse than holding no licence. Nonetheless this is not an argument against licensing but rather an argument in favour of strictly regulated licensing in which the public can place their trust.

Finally it is also worth noting that a licence will not inform a potential user whether the PI is any good at their job. The licence simply establishes a baseline that in the eyes of the state (assuming it is the state that confers this particular authority) the PI is trusted, competent and accountable.

6.4.3 Authority and Journalism

If the case of infants demonstrates the value of authority and the case of PIs the importance of conferral, the third case will demonstrate the importance of trust and accountability. This is the case of investigative journalism as illustrated by the examples of Christopher Jefferies and of phone hacking.

Christopher Jefferies was accused of killing Joanna Yeates in Bristol in the winter of 2009. Yeates' landlord, Jefferies was arrested shortly after her body was discovered. He was released on bail and subsequently dropped from the list of suspects. Although he was never charged, certain journalists became aware of Jefferies' identity and published it. The result was that Jefferies was treated in public and by the press as if tried and found guilty. Although the press did not go so far as to state that he *was* guilty of killing Yeates his character was examined with a fine-tooth comb and his flaws presented for all to see. He was subsequently awarded damages for defamation appearing in 40 articles published by eight newspapers (Kane 2011).

The case of phone hacking in the UK was more prolonged than the Jefferies case in both its development and aftermath. It seems to have begun in 2002 with journalists at a British newspaper hacking the voicemail account of the phone belonging to Millie Dowler, a teenager who had gone missing. The practice came to light in 2006 when a PI and journalist were arrested and later convicted for illegally gaining access to information about the British Royal Family. At the time accusations were made against the same newspaper that the voicemail accounts of various celebrities had also been accessed and used for newspaper articles. In July 2011 the news broke regarding the Millie Dowler phone hacking. This led to further revelations regarding the voicemail accounts of others and the eventually closing of the newspaper at the centre of the practice later that year.

As with PIs, it is reasonable to claim that surveillance is a necessity of the job for at least some journalists. This is most clearly the case when considering investigative journalists. Therefore journalism is, at least in some forms, an appropriate role for surveillance. As such the person to fill this role should also be appropriate in the sense of being trusted to make good and responsible decisions, and held accountable. However, in both the cases of Jefferies and phone hacking there were problems with the trustworthiness of journalists leading to a reducing of their trustedness in society.

In the case of Christopher Jefferies, journalists were given privileged information in being told his name while he was still a suspect. Certain journalists then demonstrated a lack of trustworthiness in revealing his name to the public. As noted, the individuals responsible for this were held accountable and the newspapers which published the information fined.

In the case of phone hacking journalists again gained privileged information, although in this case they sought it out themselves rather than being receiving it from the police. More than in the Jefferies case, the problem here lay in journalists' use of surveillance techniques to gather information. In so doing they demonstrated a lack of trustworthiness in using inappropriate methods of surveillance. Again individuals were held accountable by courts and the one paper at which these practices were known to be systemic ceased publication.

It is worth noting that in both cases the overall system of accountability worked. The journalists were discovered, albeit after a number of years in phone hacking, and held accountable. Where imprisonment was an appropriate sanction this was employed, and in the less severe case of Jefferies the sanction was limited to fines. A further sanction could have been to prevent the journalists from acting in that capacity for money in the future. Although, like PIs, journalists are not licensed as such, they can claim conferred authority through membership of the National Union of Journalists (NUJ). The revocation of this membership could then be used as a sanction by the NUJ to reinforce the importance of trust and accountability among its members.

6.5 Conclusion

It is intriguing that so few have commented on the role of authority in surveillance. As I argued in the introduction to this chapter, none of the existing philosophical writings of which I am aware specifically calls for a surveillant to be in a position of authority in order to justify their surveillance. The final section of this chapter, though, demonstrates the difference that the concept of authority can have in clarifying the morality of a particular act of surveillance. While authority is not necessary to justify surveillance it is morally significant. Without authority, determining the morality of the above cases would be considerably harder if not impossible.

I have argued in this chapter that there is a need in surveillance to establish an authority who should carry out that surveillance. For the most part it would be wrong for "just anyone" to carry out surveillance, although there are exceptions in which a person who is not an authority may nonetheless act permissibly in carrying out surveillance. The decisions of the authority should be open in order to keep the authority accountable.

Authority helps to distinguish appropriate from inappropriate users of surveillance. I conclude that the authority to carry out surveillance is based on a person who is trusted and held accountable occupying a role which is not unethical and for which surveillance is necessary, operating within a context-defined scope, and who has had the role of authority conferred upon him or her by a suitable entity.

There are still qualifications imposed on the freedom of the authority to carry out surveillance. The most obvious of these are the further requirements of ethical surveillance. Hence the surveillance must have a justified cause, the intention behind the surveillance must be correct, the surveillance needs to be a proportionate response to the occasioning cause, it must also be necessary and stand a chance of success. Finally, the method of surveillance needs to be both discriminating and proportionate.

7. Necessity

Writing about the BBC's use of private investigators in 2011 David Jordan, the BBC's Director of Editorial Policy and Standards, claimed that "consumer investigation programmes, where we have already established *prima facie* evidence of wrongdoing, may sometimes have difficulty in establishing the whereabouts of rogues, whose misdemeanours they have uncovered, so that they can confront them with allegations of that wrongdoing. We might employ third parties to carry out the *necessary surveillance* to find out where they are and where they might be approached and, on occasion, to obtain a photograph of them [emphasis added]" (Jordan 2011). A year later, the Free Software Foundation wrote that the proposed UK Cyber and Intelligence Sharing and Protection Act [CISPA] would "give the government new powers to read, watch and listen to everything we do on the Internet. The folks behind CISPA claim that national security interests make this surveillance *necessary*, but the bill's language is so vague and overreaching that it opens the door for rampant abuse of our online rights, including bypassing privacy protections to spy on your emails and text messages, block access to particular web sites and permit companies to hand over social networking and cellphone contact lists [emphasis added]" (Lee 2012).

Both the BBC and the Free Software Foundation hence believe that it is important that surveillance, in order to be justifiable, be in some way "necessary". In this chapter I examine what it means for surveillance to be necessary, and to what extent this notion of necessity should itself be a necessary condition for surveillance.

The understanding that surveillance should be necessary is not limited to the BBC and the Free Software Foundation, but is a common feature in attempts to clarify permissible surveillance. Graham Sewell and James Barker list it as a desirable criterion, as does John Kleinig, although he refers to it as "securing the ends in a less invasive manner" (Kleinig 2009 p. 204; Sewell & Barker 2001). Article 8 of the European Union Convention of Human Rights states that "there shall be no interference by a public authority with the exercise of this right [to privacy] except such as is in accordance with the law and is *necessary in a democratic society* in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the

protection of health or morals, or for the protection of the rights and freedoms of others [emphasis added]" (Council of Europe 1950). It is noteworthy that in British law, the Regulation of Investigatory Powers Act (2000) invokes the need for surveillance to be necessary. It states that, "the matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought *necessary* to obtain under the warrant could reasonably be obtained by other means [emphasis added]" (Regulation of Investigatory Powers Act 2000).

Despite this commonality of vision amongst journalists, activists, philosophers, management theorists and law-makers it remains unclear as to what exactly is meant by the requirement that surveillance be necessary. A similar quandary exists in the just war tradition regarding a frequently-held stipulation that war be a matter of "last resort". I take "last resort" in this instance to be tantamount to "necessary". So when, if ever, does war become necessary? Is it when a neighbouring state engages in sabre rattling along your border, when they cross your border and invade your territory (but might return home), or when they enter your capital city?

In this chapter I consider necessity as it affects surveillance. Firstly I look at definitions of necessity in an attempt to understand the usage of necessity which is called for in these cases. There are numerous different usages of necessity, and not all of them will fit this account, as shall become apparent. In this discussion I shall also address the question of what the action is necessary *for*. It seems meaningless to ask whether surveillance is necessary without first establishing what it is attempting to achieve. Secondly, I look at what it is that renders X necessary, when X is an act of surveillance. I then distinguish the relationship between necessity, proportionality and just cause. Finally, I argue that necessity is itself a necessary condition for justifiable surveillance.

7.1 Defining Necessity

There are several different usages of the term "necessary". There is first a logical usage. Conditions, for example, may be termed necessary and/or sufficient. While this is used in the phrase "being a fox is a necessary condition for being a vixen," it is clearly not the

usage implied in the normative statement "surveillance should be necessary for it to be permissible."

A second usage of necessity is in terms of properties. Here necessity is contrasted with contingency. An apple remains an apple no matter whether it is red, yellow or green. Philosophers have sometimes argued that there may a necessary essence belonging to "appleness" while the colour of an apple is contingent. However, it is again clear that it is not this sense of necessity to which appeal is being made in calling for surveillance to be necessary.

A third usage of necessity is in terms of metaphysical and physical necessity. Metaphysical necessity concerns *a priori* definitions. It is metaphysically necessary that a bachelor be an unmarried man. It is not metaphysically necessary that if I drop an object it will fall. Rather this latter fact is physically necessary given the condition of gravity. Once more, this is not the usage implied when it is said that surveillance should be necessary: it is neither a matter of metaphysical nor physical necessity.

A fourth usage of necessity is in terms of means-end, or conditional necessity.[11] Hence *if* I want to do X *then* it is necessary to do Y. If I want to go to the office then it is necessary for me to get out of bed. I simply cannot go to the office without first getting out of bed, and so getting up becomes a necessary action to achieve the desired end. This is the usage of necessity to which appeal is made in saying that surveillance should be necessary in order to be justified.

To give an example, it could be that surveillance is the only possible means of gathering evidence. It follows that, *if* evidence is to be gathered *then* it is necessary that it be gathered using surveillance. There may indeed be cases in which surveillance is the only means of gathering evidence, but there will be others in which alternatives are conceivable, from interviewing people to kicking down their front door and invading their property.

[11] Boethius made the distinction between simple and conditional necessity to distinguish between an act that couldn't be avoided as it is one made of a being's nature and one that was made as a result of free will (Boethius 1969 pp. 119–129). While there are similarities in my description insofar as the necessity is a result of desiring to move from one state to another I am not using the term in its Boethian sense here.

Where there are other means then it may be that surveillance is not necessary. Necessity as I am using it here, then, refers to this notion of the relation between a means and its end.

This being the case, it becomes important to question the end to which surveillance is the necessary means. It may be that the end is gathering information. This seems like a reasonable end for surveillance. How, though, would it be known if gathering information were justified? The end in mind, in order to be justified and if it is not itself justified by necessity, should be covered by one of the other principles of just surveillance, and indeed it is. The end is provided by the principle of just cause. The just cause presents the end to which the surveillance is justified, and hence also the end to which it must be asked whether surveillance is necessary. Hence the question becomes: if I am justified in treating X as liable for surveillance then is it necessary that surveillance is used to prevent X from a particular action or prove that X was responsible for a particular action.

Having established what is meant by necessity, the next consideration is when an act becomes necessary. Through looking at this the value of necessity will become apparent.

7.2 When is an Act Necessary?

Writing in the just war tradition, John Lango has identified two conditions of necessity (or "last resort", which is how necessity is typically referred to in that tradition) which fit with what I have so far said on the subject. These conditions are feasibility and awfulness (Lango 2006). The feasibility condition states that an act is necessary if there are no feasible alternatives. The awfulness condition states that an act is necessary if the alternatives are more harmful than the act under consideration. Lango argues that when one of these criteria is met then the action under consideration may be deemed necessary. I shall now consider each of these conditions in greater depth as they apply to surveillance.

7.2.1 Feasibility

Lango describes feasibility in terms of just war as it not being "reasonable to continue to attempt to end the conflict through negotiations. … That it is not reasonable to attempt an alternative measure before using armed force" (Lango 2006). That is, there are no reasonable alternatives to the measure that is being proposed. In Lango's example, the alternatives to using armed force are negotiations, but these are not reasonable (the

implication in Lango's example being that they have been tried and have not succeeded, or do not show signs of being likely to succeed).

What does it mean for there to be no feasible alternatives to surveillance? It is arguable that there is always *an* alternative to surveillance, namely no surveillance. However, is this a *feasible* alternative? That is, can the ends still be achieved without using surveillance? If so, then "no surveillance" is a feasible alternative to surveillance. If not, then "no surveillance" is not a *feasible* alternative.

7.2.2 Awfulness

The second of Lango's conditions is awfulness. He argues that an act is necessary if the alternatives (including the results of not performing the act) are more harmful than the act itself. I have looked at the harms of surveillance in chapter 3, but it is helpful to consider alternatives to surveillance which could elicit similar information to see which are more and which less harmful.

Starting with those alternatives that are more harmful than surveillance, the list is quite long. Rather than merely monitor someone, one could intrude more forcibly into that person's life, for example entering that person's property either when they are there or not and searching for evidence which might otherwise have been discovered by less intrusive surveillance. Similarly, searches could be carried out on the individual themselves, such as when suspected drug smugglers are strip searched at airports. More harmful still would be the arrest of a person so that their liberty is restricted and they can be questioned at length by the police. Within this context there are then different means of questioning a suspect, from standard questioning to more "hard nosed" interrogation techniques, to the employment of methods of intimidation and torture. Each of these, in most circumstances, would be more harmful, certainly to an individual and probably to society at large, than surveillance. As such, if the only choice available to achieve a justified goal is between surveillance and torture, surveillance would be classed as necessary according to this condition. To use Lango's terms, surveillance would be "less awful" than torture.

In contrast to methods more harmful than surveillance are those that are less harmful but which might achieve the same ends. The alternatives here seem to be doing nothing (the

"no surveillance" option discussed above) or gentle but persistent questioning, typical of television detectives such as Columbo. The fact that there are fewer less harmful alternatives to surveillance is quite telling. It suggests that, once a goal has been justified, surveillance may be one of the less harmful means of achieving that goal.

It should be noted here that this discussion concerns the role of surveillance *per se*, and not any particular form of surveillance, which would be a matter of means and hence relevant for consideration as a factor of *jus in speculando*. There are some types of surveillance which are more intrusive than others (see chapters 10 and 11) and some which are less discriminating than others (see chapter 12). While surveillance may be a necessary response, then, a particular *form* of surveillance may not be necessary.

This can be illustrated with the example of using CCTV in high school toilets to identify school bullies (W. Johnson 2012). In situations in which bullying is restricted to school toilets, a typically private area in which this activity can thrive, surveillance may be deemed necessary. Asking pupils whether they are being bullied (or bullying others) is less harmful but also less likely to be effective. For the sake of the illustration let us assume that every pupil has been asked and replied in the negative. Despite this, evidence remains of bullying taking place in the toilets. A total absence of surveillance would be neglectful of a duty of care to the pupils, particularly the victims of the bullies. Hence surveillance *per se* is necessary.

While surveillance *per se* is necessary in this example, the method of surveillance still needs to be determined. CCTV, as indiscriminate, will record the passing of all pupils in the toilets and not limit itself to those broadly seen as being at risk. In this case a more discriminating approach might be preferable to avoid giving all pupils the sense of being watched when they enter the toilets. At the same time it could be argued that this prevents discrimination *against* certain pupils on the basis of their age, colour, looks, history, etc. and so might prove to be more justifiable than more discriminating methods (Hadjimatheou 2013). Turning to proportionality, CCTV when used in public is generally not intrusive: it captures images available to anyone on or just watching the street (Ryberg 2007). In the confined space of school toilets, though, CCTV monitors behaviour which is usually taken to be private (in the stalls) or semi-private (in the rest of the toilet area) when one is frequently aware who else is present in the room. Furthermore, its ability to record and

store high-quality images of this private/semi-private space for indeterminate lengths of time means that it is intrusive in this situation.

In contrast with CCTV, a teacher or teaching assistant could be stationed at the school toilets, tasked with monitoring who enters and leaves the room. Granted there is a danger of discrimination against some pupils by the teacher, but assuming a level of professionalism by that teacher this should not occur. The teacher then has the freedom to enter the room if a person has raised his or her suspicions, but need not be permanently in the room to avoid giving pupils the sense of being watched. Finally the teacher does not have the same capacity to record and share images as does a CCTV system. In summary, while surveillance could be necessary in school toilets for this reason, it is hard to justify CCTV as the means of surveillance when there are more discriminating and less intrusive measures available.

7.3 Necessity, Just Cause and Proportionality

It would be helpful at this point to clarify the relationship between necessity, just cause and proportionality. Each is related but importantly different, hence requiring a different principle in the overall scheme of just surveillance.

It may be easiest to approach this through an example. Imagine I know that Squirt, an alien on a nearby planet, is planning to kill me for his amusement (I have done nothing wrong) by firing a very accurate laser from his planet to the Earth such that it will kill me and only me. Under these circumstances and the principle of self-defence, I would have a just cause in acting to prevent Squirt killing me.

Imagine that in order to prevent Squirt killing me, the only option available to me is to kill Squirt (Scenario 1). He is so set on ridding the universe of me that only his death will save me. If this is the case then I have a just cause to kill Squirt (preventing him from killing me) and it is necessary for me to kill Squirt in order to achieve that just cause (i.e. there are no feasible alternatives available to me).

Imagine now instead that in order to prevent Squirt killing me I need simply say, “Abracadabra” three times (Scenario 2). Squirt is very superstitious and has very good eavesdropping equipment. On hearing me say this he will drop his plans to kill me. In this

case I have a just cause to kill Squirt (preventing him from killing me) but it is not necessary for me to kill him in order to achieve that just cause. There is a feasible alternative and it is less awful than killing Squirt.

This separates just cause from necessity. In order for an act to be permissible it must have a just cause. That just cause then provides an end by which the act can be assessed in terms of necessity. Necessity is an issue of whether the act is the only way, and whether it is the least awful way, of achieving the justified end. What, though, of proportionality?

Let us return to Scenario 1, the "kill Squirt" option. In this case there are a further two options. Option 1 is that I have a laser similar to Squirt's which can single him out and kill him and only him. Option 2 is that I do not have such a laser but instead a very large rocket tipped with sufficient nuclear warheads to destroy his entire planet, including the 7bn aliens like Squirt living on that planet.

I have already said that in Scenario 1 I have a just cause to kill Squirt and it is necessary for me to kill Squirt. In option 1 it is also proportionate that I kill Squirt. It is a simple trade-off of his life for mine, which is proportionate (I am presuming here that Squirt's life and my own are of equal value). Hence in Scenario 1, Option 1 killing Squirt has a just cause, it is necessary and it is proportionate.

In Option 2, though, it is not proportionate that I kill Squirt. His death will necessarily be accompanied by the destruction of his planet and the deaths of 7bn aliens. Continuing the assumption that Squirt and the other aliens on his planet have lives of equal value to humans then to kill Squirt would not be proportionate. Hence in Scenario 1, Option 2 killing Squirt has a just cause, it is necessary but it is not proportionate.

Returning now to Scenario 2 ("superstitious Squirt"), there are again a further two options similar to Scenario 1. I may kill Squirt with an accurate laser (Option 1) or I may destroy his planet and the other aliens living thereon (Option 2). In Scenario 2, Option 1 I have a just cause to kill Squirt, it is not necessary that I kill Squirt (there is a less awful alternative), but it is proportionate (a life for a life) if I do kill Squirt. In Scenario 2, Option 2 I have a just cause to kill Squirt, it is not necessary that I kill Squirt and it is not proportionate that I kill Squirt.

From this discussion it can be seen that, while just cause, necessity and proportionality are related they can come apart. It is possible to have a just cause to act but no necessity and the act would be disproportionate (Scenario 2, Option 2). It is also possible to have a just cause to act and necessity but the act be disproportionate (Scenario 1, Option 2) and to have a just cause to act and no necessity but the act be proportionate (Scenario 2, Option 1). Finally it is of course possible to have just cause, necessity and the act be proportionate (Scenario 1, Option 1).

One further aspect that this analysis highlights is that necessity can refer to both ends and means. It seems reasonable to ask if it is necessary to kill Squirt (ends) but if I have a choice between using the laser or the rocket then I can also ask whether it is necessary to kill Squirt *using the rocket*. The answer here is clearly no, as there is a less awful alternative (using the laser). Of course, either is equally awful for Squirt, but in the greater scheme of things it is less awful for the 7bn other aliens that it is just Squirt that is killed.

This provides a challenge to traditional just war schema, at least as it is portrayed by some. Typically just war thinking considers necessity as an aspect of *jus ad bellum* but not *jus in bello* (Orend 2000 p. 134; Coates 1997 p. 208; G. Graham 1996 p. 57). *Jus in bello* consists primarily of the principles of proportionality and discrimination. Some authors do consider necessity as a condition for *jus in bello* (Frowe 2011b pp. 106–07; Hurka 2005) but this is not universal. Others appear to consider necessity a part of the principle of proportionality (Coady 2007 pp. 110–11). The analysis above suggests that necessity should indeed be a third consideration in terms of *jus in bello* as well as *jus ad bellum*.

To illustrate this, necessity as a condition of *jus ad bellum* can be applied to the declaration of war on Japan by the US and Great Britain in 1941 and as a condition of *jus in bello* it can be applied to the subsequent dropping of the atomic bombs on Hiroshima and Nagasaki in 1945. In terms of *jus ad bellum*, it should be asked whether war was a necessary response to the actions taken by the Japanese in bombing Pearl Harbour and allying themselves with a state with whom Britain was already at war. That is, were there feasible alternatives and were these alternatives more or less awful than the declaration of war?

Turning now to the dropping of the atomic bombs (a consideration for *jus in bello*), it can be asked both whether these acts were proportionate *and* whether they were necessary. I

have demonstrated above that these two considerations can be dealt with separately. Hence it is possible for the bombings to be proportionate and necessary, proportionate but not necessary, not proportionate but necessary, or neither proportionate nor necessary.

This same picture carries across to just surveillance. I have treated it here in the section on *jus ad speculandum*, but there is an argument to be made that it should also be a consideration of *jus in speculando*. I do not have the space in this thesis to do this, but acknowledge that it is a weakness in the overall schema of both just war and just surveillance thinking if necessity is not taken to be an aspect of both ends and means.

7.4 Is Necessity Necessary?

Having established the definition of necessity, conditions for necessity and distinguished necessity from just cause and proportionality, it remains to be asked whether necessity is itself a necessary condition for just surveillance. To answer this I return to the fact that necessity is typically referred to in the just war tradition as "last resort". Indeed, it is in these terms that Lango writes his conditions for necessity.

My reason for using the term necessity over last resort was that the use of "last" was unclear. At what stage does something become a last resort? Furthermore, as noted in the introduction, necessity is a phrase which is often used to describe a desirable condition for surveillance (Kleinig 2009; Sewell & Barker 2001; RIPA 2000). The final question of this chapter is hence whether necessity is merely desirable or if it is in fact a necessary condition.

While the notion of last resort is unclear, it does hold an important implication which is lost in translation to "necessity". This is the caution against premature use. That is, surveillance could be employed too readily when less harmful alternatives (as defined in terms of Lango's analysis) exist. Given the harms that are attendant upon surveillance (see chapter 3) it would be wrong for surveillance to be employed prematurely, if, as noted, there are feasible and less awful alternatives available. As such, it is correct that necessity, as a consideration of those alternatives, be a necessary condition for just surveillance.

7.5 Conclusion

Authors, declarations and laws have contended that necessity is an important condition for surveillance to be justified. However, it has not always been clear what necessity entails.

I have argued that necessity in the case of surveillance concerns the means to achieve an end. This end, I claimed, should be the just cause for the act of surveillance. I suggested also that a comparison could helpfully be drawn with the just war tradition in which necessity is often described as last resort. Here I drew on the work of John Lango to argue that there are two conditions: feasibility and awfulness. Feasibility holds that an act is necessary if there is no feasible alternative. Awfulness holds that an act is necessary if it is less harmful than the available alternatives.

I then clarified the relationship between just cause, necessity and proportionality. In so doing I noted that it is important to consider necessity as it relates to the ends of an act of war or of surveillance. However, I also argued that it is a relevant consideration in relation to the means of an act of war or of surveillance. This demonstrates an omission in the writings of at least some commentators on the just war tradition who tend to see necessity purely in terms of *jus ad bellum*, when it should also be an aspect of *jus in bello*, and is therefore a salutary lesson for considerations of *jus in speculando* as well as *jus ad speculandum*.

Finally, drawing on the parallel with last resort as a condition of just war thinking, I argued that necessity is a necessary condition of just surveillance. Without a consideration of necessity there would be insufficient consideration of alternatives and a risk of employing a harmful action (surveillance) prematurely. The condition of necessity is a precaution against this occurring.

8. Declaration

The Just War Tradition, on which this thesis draws, includes a principle of declaration. That is, in order to be permissible, a war should be openly declared as such. Is the same true of surveillance? This chapter seeks to determine how could, and if so where should, a principle of declaration apply to surveillance.

There are several questions which arise from bringing the principle of declaration into the ethics of surveillance, each of which this chapter addresses. First I look at the purpose (if any) of a principle of declaration when it comes to surveillance. I then turn to what and how much needs to be declared in this context. Thirdly I consider to whom the surveillance should be declared. Should it always be declared to the surveilled subject or may there be others to whom it should be declared? Finally, I ask whether declaration is a necessary condition of surveillance.

8.1 Why Declare Anything?

Imagine that Daniel and Edward are walking through a wood one morning with Daniel's dog. Following a stick thrown for him, the dog disappears into the undergrowth and fails to return. Wondering what has happened to his dog, Daniel beats his way through the undergrowth to find his faithful companion standing over a dead human body. Wanting to determine the identity of the dead person, Daniel quickly searches the body, finds a wallet and opens it. At this moment, having been wondering what has happened, Edward walks over to see Daniel rifling through the pockets of a dead person and apparently stealing money.

How Edward reacts at this point will of course depend largely on how well he knows Daniel and Daniel's character, and what sort of a person Edward is. Were they both cold-hearted thieves then Edward might approve what he sees and demand a share of the takings. If Edward is more upright but suspects Daniel of being a cold-hearted thief then he may accuse Daniel of stealing from the dead. If Edward is the cold-hearted thief and Daniel the more upright then Edward may try to persuade Daniel to give him the wallet. Finally if both are morally respectable citizens then Edward will likely give Daniel the benefit of the

doubt and accept his explanation of looking for identification (although he may begin to harbour some doubts about Daniel...).

This situation is unlikely (why the need to identify the body instead of just informing the police?) but it draws on an accepted social practice that if a person finds himself in this position, then he should tell a witness that he is looking for identification before rifling through the pockets of the dead. That is to say, he should declare his intention.

In this case, Daniel's interest in declaring his intention before looking for the wallet is primarily prudential. By not making a declaration to Edward he risks having his actions and his character called into question. There is also a moral dimension to the declaration. If he had explained his intention to Edward, Daniel would have introduced an element of accountability to his action. If he had said he was looking for identification, and sought Edward's oversight, then he may have been less tempted to take any money that was in the wallet. Finally, it is worth noting that the person to whom the declaration is made is significant. It is better to declare to a witness of upright character than one of more dubious inclinations. Accountability is worth little if the person to whom one is accountable, and who may be called upon to give witness to one's character, is himself of questionable moral character.

The case of the dead body in the woods is interesting in terms of the importance of declaring intent, but not directly applicable to surveillance and not particularly moral in terms of argument. A case which is more pertinent to surveillance, morality, and the importance of declaration would be that of the police entering a private property. There is a significant difference between the police entering the property with a warrant and their doing the same without a warrant. The warrant declares that the police are accountable in what they do to a higher body (a judge). Once more there are prudential reasons for insisting that the police require a warrant before entering private property, not least because the alternative could amount to a police state in which any property might be entered at whim. However, the moral reason of accountability is in this case at least as important as the prudential, if not more so. A single case of the police entering a property without a warrant would not render the country a police state, but it would be an instance of the police acting inappropriately without accountability.

A different picture emerges, if one looks at the case of speeding cameras, at least as they are currently used in the UK. These are painted bright yellow, are preceded by signs warning that speeding cameras are in use, and can be detected from obvious markings on the roads indicating their presence. There are also road atlases and automated GPS systems which alert drivers to the presence of these cameras. In all, it is hard to imagine what more could be done to declare the existence of these cameras to drivers.

The justification for declaring the presence of the speeding cameras is importantly different in a number of ways from that of the police gaining a warrant. In the first place, the police make their declaration to a higher authority whose property will not be invaded. The speeding cameras, in contrast, make their declaration to the surveilled subject. Secondly, the police make their declarations (presuming they do) in such a way that they will gain accountability. There may be some level of accountability needed for speeding cameras (i.e. that they are calibrated correctly and not just being used to make money for the owners of the cameras). However, the central reason for declaring the presence of the speeding cameras is surely to change the behaviour of the (potentially) surveilled subject. Knowing of the cameras' presence, the surveilled subject will likely either slow her driving or drive via a different route which avoids cameras altogether.

Yet another picture emerges in looking at surveillance in the corporate world. Many telephone conversations with customer sales representatives or help staff are preceded by a declaration that, "this call may be monitored for training purposes," or, "to improve our service." In this case the stated aim of the surveillance is clear, but why the declaration? The *declaration* is not necessary for the training of staff. In many cases there is doubtless a legal requirement, but the question then arises as to why should there be such a requirement. There are several reasons why the declaration may be important in this context:

- it may dissuade customers on the phone from becoming aggressive, in the knowledge that if they do there will be a record of the aggression;
- it may imply that by hearing the declaration and continuing with the call the customer gives her consent to the recording and hence the surveillance becomes consenting. If the customer does not consent then she can end the call;

- it may stem from an assumption that people's conversations are by default private between those people. If there is to be a deviation from this default then we have an expectation to know about it and to know why;
- it may relate to the use to which the recording is put. If it is later used in advertising, for example, then the customer may complain that this is not what she consented to.

Of these reasons, the first two relate to a change in behaviour. The customer either does not act in a way that she might have acted had the recording not been in place, or the non-consenting customer ends the call rather than continue and be recorded. The second two relate to accountability. The company has a duty to the customer to explain that a conversation is being recorded and why, and the customer can then hold the company accountable as to the use of the recording (at least to a degree – the customer may not always know the use to which the recording has been put).

In my final case, again in the corporate world, some supermarkets carry out surveillance on their customers through both CCTV and customer loyalty cards. In the case of CCTV there may be a desire to affect behaviour of potential shoplifters, but the cameras also enable the shop to monitor the behaviour of their customers. The same is true of loyalty cards. In both of these cases it is important to the supermarket that the customer does *not* change his behaviour. Rather the supermarket wants to record that behaviour in a way that enables it to better understand the customer and so sell him more, or more expensive, goods.

In the case of supermarkets, then, the reasons for declaring the surveillance are manifold. However, they do map onto at least some of the reasons given for declaring the recording of phone conversations. Hence supermarkets may declare the surveillance because:

- it may dissuade potential shoplifters from stealing, in the knowledge that if they do there will be a record of the act;
- it may imply that by seeing the signs and continuing to use the supermarket the customer gives his consent to the recording and hence the surveillance becomes consenting. If the customer does not consent then he can (at least in theory) shop elsewhere;

- it may relate to the use to which the recording is put. If it is later used in advertising, for example, then the customer may complain that this is not what he consented to.

The one area in which there is not an obvious correlation is in the assumption that people's conversations/trips to the supermarket are private by default. Going shopping in a public place is not a private activity, although *what* a person purchases may be considered at least more private than the fact that they are in the supermarket. There is also an assumption that people's shopping trips are not *recorded* (as opposed to being private). These two things imply that there is a correlation in the following way:

- it may stem from an assumption that people's shopping trips and the content of their shopping baskets are by default not recorded. If there is to be a deviation from this default then there is an expectation to know about it and to know why.

This being the case there are again the same reasons for declaring surveillance in the case of supermarkets as in the case of telephone calls. These are a combination of changing (some) behaviour, becoming accountable, and seeking consent.

From these cases it is possible to draw the conclusion that there are at least three purposes for declaring surveillance. The first is to gain accountability of the surveillant. The second is to change the behaviour of the surveilled subject. The third is to gain the consent of the surveilled subject. The questions then arise: to whom should declarations be made and whether the purposes of the surveillance can be in any way tied to this person.

8.2 Declared to Whom?

Along with suggesting that there are three purposes for declaring surveillance, I have also suggested that there are two possible entities to whom the surveillance could be declared. These are the surveilled subject and a higher authority. In this section I will look at these in more depth to understand them more fully and see whether there is a connection between the person to whom the declaration is made and the purpose of the declaration.

8.2.1 Surveilled Subject

It is not uncommon for people under surveillance to know that they are such. CCTV is a frequent feature in British urban environments, and well-publicised statistics suggest that the average Londoner may appear on CCTV cameras 300 times in a day (Frith 2004; McCahill & C Norris 2003). Yet the cameras are often not hidden. Indeed, there are frequently large signs in place to inform those who may be filmed by the cameras that there are such cameras in operation in that area. This is also true in the case of surveillance carried out in supermarkets, as noted above.

This declaration of the presence and use of CCTV cameras is similar to that of speeding cameras. In both cases the declaration is made to the surveilled subject. In both cases there is a deterrent effect to potential wrongdoers (i.e. do not speed/shoplift here or you will be caught). That is, there is a desire to affect the behaviour of at least some of those being surveilled. There is also a possible motive of gaining the implicit consent of the surveilled subject, such that the fact of the surveillance becomes less ethically problematic.

The declaration made to the surveilled subject may, as noted above, also serve to introduce an element of accountability to the surveillant. Film taken of a supermarket customer having an embarrassing but otherwise harmless accident should not be submitted to a television programme specialising in showing such film without the permission of the customer(s) involved. By implicitly agreeing to being filmed the customer may have given this permission only insofar as the film is used to counter crime and improve customers' shopping experiences, but not for purposes of entertainment.

8.2.2 Higher Authority

I have argued that the declaration may be made to a higher authority, in cases such as the police seeking a warrant to enter someone's property. In this case, a declaration to the surveilled subject would most likely change their behaviour, which would defeat the purpose of the surveillance. If the police alerted a suspected drug pusher that they wanted to place him under surveillance, he would most likely suspend any illegal operations while that surveillance was in place.

The same would be true of an investigative journalist working to reveal a government cover-up. If those in government knew that the journalist were investigating their activities then they might suspend those activities or make them harder to identify. In certain chilling scenarios some in authority might even try to kill the journalist, as was rumoured to be the case with Anna Politkovskaya (Amnesty International 2011; Simpson 2006).

Presuming that catching drug dealers and uncovering government corruption are good things, it would be wrong to insist that the surveillant declared the fact of the surveillance to the surveilled subject. This would be counter-productive and may even put the life of the surveillant at risk. In these cases it is also safe to assume that a declaration would not be a prelude to consenting surveillance. If the subject is doing something wrong then she is not likely to agree to the surveillance. Furthermore, this level of surveillance (police entering properties or investigative journalism) generally involves a greater degree of intrusion into a person's privacy than speed cameras or CCTV in public places. Hence even a person who is not guilty of any wrongdoing may have reason to refuse consent to this level of surveillance.

If a declaration could only be made to the surveilled subject then these cases would be problematic. If a declaration is not made to the surveilled subject because a) the surveillant does not want the subject to change her behaviour; and/or b) the subject is very unlikely to give consent to the surveillance, then the third benefit of giving a declaration (gaining accountability) would be lost.

To maintain accountability of the surveillant in these particular acts of surveillance it is therefore important that a declaration of the surveillance be made to *someone*. Going back to the case of Daniel and Edward, it is preferable if that person is independent and trustworthy. Hence the police approach a judge in order to secure a warrant to enter a suspect's property or listen to his phone conversations. The investigative journalist has a harder time here and must rely on his employer in order to gain a degree of accountability (Cluley 2013). In the case of freelance journalists where there is no obvious higher authority to whom they could turn before carrying out the surveillance, there is the danger that they might have their intentions misunderstood, like Edward coming across Daniel rifling through the pockets of the dead.

Where declaration cannot be made to the surveilled subject because this would jeopardize the possible success of that surveillance, a declaration should therefore be made to an independent person. I will call this person a higher authority. In more formalised settings, such as the police seeking a warrant, the nature of the higher authority is clear in that a judge is a constitutionally higher authority that the police. In less formal situations, though, the title "higher authority" still conveys important aspects. He is a higher *authority* because, by his consenting to the surveillance, the independent person offers *an element* of authorisation to that surveillance. I do not want to suggest that he can authorise the surveillance in any legal sense (unless he is a judge), nor that he can necessarily offer a full authorisation in a moral sense. However, there is a limited authorisation that he offers by agreeing to be an independent witness to the surveillance. He is a *higher* authority in the sense that he is able to offer that authorisation (however limited it may in fact be) to the surveillant. He is not implicit in the surveillance, nor is he subject to the surveillant, and so he is neither equal to nor lower than the surveillant in terms of authority over this one particular act. Further, he can withdraw his consent if the surveillant acts, or appears about to act, in a manner with which he is not comfortable. Thus by agreeing to act as an independent witness he takes on a limited position of authority over the surveillant.

I have argued that there are three reasons why a declaration of surveillance should be made: to change the behaviour of the surveilled, to gain consent of the surveilled subject, and to gain an element of accountability for the surveillant. I have also argued that the declaration can be made to either (or both) the surveilled subject and a higher authority. When the declaration is made to the surveilled subject then all three purposes for the declaration may be at work. The declaration may serve to change behaviour, gain consent and introduce accountability. When it would be counter-productive for the surveillance to be declared to the surveilled subject, because the surveillant does not want to risk changing the behaviour of that subject and/or does not believe that consent is likely to be forthcoming, it should be declared to a higher authority in order to retain the element of accountability.

8.3 What and How Much Declared?

There remains a question as to what and how much should be declared to either the surveilled subject or the higher authority. It may be that the entirety of the surveillance (every camera and microphone) should be pointed out to the subject or the authority. That

is, the *operation* is declared to the relevant entity. On the other hand, it may be that merely the possibility of the operation (through the existence of a body that could carry out such operations) is pointed out to the relevant entity. That is, the mere *existence of the surveillant* is declared.

In addition to these two variables (existence and operation) regarding what is declared, there is the question of how much is declared. Some operations, such as speed cameras and CCTV in public areas are overt. They may be there, as discussed, to alter behaviour and so it might be counter-productive to *hide* their existence and operation. Other operations may be covert, such as the wiretapping of a suspected terrorist's phone, because it could be counter-productive should the suspect become *aware* of the surveillance.

These four variables (existence, operation, covert and overt) give rise to four possible scenarios, described in Table 3. This table is helpful in clarifying the different possibilities between the four variables and enabling a clearer picture to develop as regards which, if any, operations and existences are problematic and what exactly needs to be declared. For three of the four quadrants I have used the US National Security Agency (NSA) as an example. Created in 1952, no government document referred to the Agency until 1957, and then very obliquely (Anon 2012). However, its existence was a poorly-kept secret in the wake of the Watergate scandal in the mid-1970s and the later publishing of James Bamford's *The Puzzle Palace* (Bamford 1982). Publicity efforts were made in the late-1990s and early 2000s which have meant that the existence of NSA is now widely acknowledged.

The table explores the relationship between the surveillant and the surveilled subject. In all four cases I will presume that a declaration has been made to a higher authority and hence a level of accountability is present.

		Operations	
		Covert	**Overt**
Existence	**Covert**	Body which is not known to exist using surveillance which is not known about. Used for gathering of intelligence for purposes of detection. E.g. NSA in 1970 listens to international phone calls to carry out espionage.	Body which is not known to exist using overt surveillance for ulterior purpose. Used for gathering of intelligence for purposes of detection. E.g. NSA in 1970 uses supermarket CCTV systems to monitor suspected foreign spies in the US.
	Overt	Body which is known to exist and known to use surveillance. Particular instances of surveillance use are unknown. Used for both deterring and altering behaviour and for detection. E.g. NSA in 2010 listens to international phone calls to carry out espionage.	Body which is known to exist and known to use surveillance. Particular uses of surveillance are known. Used in deterring and altering behaviour. E.g. Brightly-coloured speed cameras used by police. Helpful for deterring speeding traffic.

Table 3: Overt and Covert Operations compared with Overt and Covert Existence

8.3.1Which Options are Problematic?

If the common purpose of declaration to both surveilled subject and higher authority is that of gaining accountability then the covert existence of any body or operation is likely to be more problematic than overt existence and operation. Through being covert there will be accountability to fewer people, and so there is the potential for more wrongdoing should those people become corrupted. I take it that it is harder to corrupt more people than fewer, and so accountability will generally be higher the more people there are to which a body is held accountable. This is a generalisation. It is of course *possible* that accountability is

extremely high through a high level of vigilance when those to whom a body is accountable are few, and relatively low through a low level of vigilance when those to whom a body is accountable are many. While this is possible, though, it is less likely.

This being the case, the more covert a scenario is, the greater the likelihood of there being less accountability for the surveillant. As such, the more problematic cases are the more covert. Hence the most problematic scenario pictured above is that of a covert existence with covert operations. In this case the accountability of the body is likely to be extremely limited and the potential for abuse high.

Marginally less problematic is the case of a covert body using overt operations. This is obviously a strange scenario, but I have suggested one situation in which it might occur, namely using known surveillance equipment which is believed to belong to a different organisation. Such a scenario appears to be marginally less problematic in that the subject is at least aware of the surveillance and so there is scope for behaviour change. Nonetheless, that the subject has a limited understanding of the uses to which the surveillance material may be put means that this is still problematic.

The purpose of the declaration when made to the surveilled subject, as noted above, is to change behaviour, gain consent and/or gain accountability from that subject. In this instance, though, any change in behaviour will relate to the perceived purpose of the surveillance, rather than its true purpose. Indeed, were its true purpose known then the change in behaviour may be quite different. It is quite likely that the surveillant does not wish for this change in behaviour as it would run counter to the purpose of the surveillance. For instance, a subject may not worry about discussing politics in a supermarket whilst under the belief that the CCTV cameras present are there to catch shoplifters. If it turned out that the cameras were being used by the secret police to identify political dissidents then the change in behaviour would likely involve ending such political discussions. Secondly, it is impossible for the surveilled subject to give informed consent to the surveillance if that subject does not know of the existence of the body carrying out the surveillance.

The conclusion here is that when a covert body uses overt operations the implicit declaration to the surveilled subject of that operation made through the overt nature of the

operation is *almost* irrelevant. I say almost as there is limited scope for behaviour change and accountability of the ostensible operating body, and through the latter a discovery of the ulterior motive. However, these are unlikely under the circumstances and so this quadrant verges on being as problematic as the first.

The third option is that of a body which is overt in existence but covert in its operations. This is a common situation in liberal democracies in the 21st century in which the existence of intelligence organisations is well known, but their operations are kept a guarded secret.

In these cases the formal level of accountability may not differ much from those in which the body's existence is covert. However, the informal level of accountability is likely to be much higher. The public's knowing about the existence of an organisation means that there will likely be a greater public insistence on keeping that body accountable. Wrongdoings of a known body are more likely to come to light than those of an unknown body and so accountability to the surveilled subject is, while not necessarily the case, more likely. The known existence of the body will also likely lead to a change of behaviour in some who are tempted to wrongdoing. The potential traitor may be more likely to think twice of selling state secrets if he knows that there is a counter-espionage body in operation than if he believes that there is not. For those not tempted to wrongdoing (and even for some who are) there may also be a level of consent to the existence of the body. Its operations may be seen as necessary for the security of the state, and the fact that those operations are covert broadly appreciated to be necessary to their purpose (the apprehension of foreign spies).

The final quadrant concerns the body which is overt in existence and whose operations are overt. This may well typify the police using speed cameras on public roads in the manner to which I have already referred. Of the four quadrants this is the least problematic as there is full disclosure to the surveilled subject in advance of the surveillance to both the possibility (the existence of the surveillant body) and the likelihood (the operations of that body) of that surveillance. This allows for the three purposes of declaration to the surveilled subject to be met: possible change of behaviour, gaining of consent, and gaining of accountability.

As the options are passed through in reverse order (i.e. from overt-overt to covert-covert) there is an increasing burden of justification on the part of the surveillant for not declaring

the operation to the surveilled subject. It is not that the surveillance cannot be justified in the absence of such a declaration. Indeed, I have highlighted cases where it should *not* be declared to the surveilled subject. However, the need for such a justification becomes more necessary with covert operations and even more so with covert bodies in order to provide accountability.

8.4 Returning to Just War

Having examined the purpose for and the extent of the principle of declaration I am now in a position to return to the analogy with the just war tradition and see whether there are any parallels with the principle of declaration insofar as it pertains to war. If so, is there anything that can be learned from these parallels?

It is worth beginning with some obvious disanalogies. Firstly, war is not covert. Granted, there may be covert aspects to war (espionage, sabotage, etc.) but the war itself is extremely overt. Hence while some operations of war may be covert, the existence of the war, and the warring parties, is overt. Secondly, while a declaration of war is, as noted, considered to be important in the just war tradition, that declaration is generally not intended to gain accountability of the warring parties. Such accountability should be provided by the international community, although in practice it is often carried out by the victor towards the loser in war.

Despite these disanalogies, though, there are many similarities. At least since the founding of the United Nations there has been an effort made to introduce a higher authority into the domain of warfare. Hence it is often taken that declarations of war should pass through the UN Security Council in order to be legitimate. This is not necessarily the case, but that there is scope for the UN Security Council to act as a higher authority is a parallel.

The notion of a higher authority is not a purely contemporary phenomenon, either. The principle goes back at least to the Roman empire, in which a body of priests called the *fetiales* met to discuss the legality of a proposed war before that proposition was taken to the Senate. The *fetiales* therefore declared to the Senate that war could legally be undertaken. Cicero, who sought to provide philosophical basis for the Roman laws of war,

wrote that no war is just "unless it has been formally announced and declared beforehand" (Cicero 2006 p. 52).

The *fetiales* and Cicero establish that the principle of formal declaration has a long heritage. It is not until the modern period, though, that the reason for the principle of formal declaration has been discussed. From Cicero and the actions of the *fetiales* it may be assumed that in ancient Rome the purpose was to ensure the legality of the war. A contemporary version of this would be holding the cause of war to juridical and public account. However, Hugo Grotius disputes that this is the purpose of the principle of declaration, arguing instead that the purpose of the principle concerns the legitimacy of the authority declaring war rather than the cause of that war. He writes, "the reason why nations required a declaration for the kind of war which we have called just according to the law of nations was not that which some adduce, with the purpose that nothing should be done secretly or deceitfully. … The purpose was, rather, that the fact might be established with certainty that war was being waged not by private initiative but by the will of each of the two peoples or of their heads" (Grotius 2006 p. 424). Hence the principle ensures that war is waged by the correct authority. Writing in the 20th century, the Council of US Bishops agreed with this view, treating the issue as a part of the broader principle of authority, rather than relating to the just cause (National Conference of Catholic Bishops 2006 pp. 671–72).

It may seem paradoxical to talk about consent in war, insofar as no-one (or at least very few) *wants* to go to war, but the declaration of war does serve to establish an agreement between two states that they are at war. War is declared by one state and accepted by another. There is at least an element of this in the above quote by Grotius: if war is not declared then there was no means of ascertaining that it is being waged by legitimate authorities, rather than by private armies posing as those authorities.

Finally, a declaration of war may also be undertaken to change an adversary's behaviour. An obvious example of this would be the 1991 declaration of war against Iraq in which the aim was to get Iraq to end its illegal occupation of Kuwait. The UK's declaration of war against Germany in 1939 may also be seen as an attempt to end the latter's policy of expansion into neighbouring states (or at least the neighbouring state of Poland). From the

perspective of a state fighting for its defence there is typically a desire to end the aggressive behaviour of the invading state.

Hence there are parallels between the need for a declaration of war and of surveillance. While war is always overt to those who are involved (although particular operations may be covert), the purpose of the declaration and the bodies to whom the declaration should be made (the warred against and/or a higher authority) are broadly similar. When the declaration is made to a higher authority this gains a degree of accountability for the declaration of the war, the declaration can also gain a degree of consent between the relevant parties that they are at war. Thirdly, the declaration of war may be employed as a means of changing the behaviour of those involved.

8.5 A Necessary Condition?

Cicero believed that it was necessary for war to be declared in order that it be permissible, and the importance of declaration in just wars has carried through the centuries to the Council of US Bishops in the 20th century. This raises the question of the position of the declaration in a system of just surveillance: is it a necessary or *pro tanto* requirement of surveillance?

I have argued that the declaration may be made either to a higher authority and/or the surveilled subject, and that the common purpose of the declaration in both cases is to gain a degree of accountability. While this is a good thing, it is not, I believe, absolutely necessary. Hence there may be acts of surveillance which are justified even when no declaration has been made.

To argue for this I will consider two cases. One involves returning to Daniel and Edward in the woods with the dead body. Imagine that prior to Daniel finding the body Edward had had to leave the woods in a hurry, such that Daniel continued the walk alone with his dog. After Edward left, Daniel discovered the dead body. In this case there was no person to whom Daniel could have made a declaration if he had tried. Assuming that he was justified in discovering the identity of the body, though, it would seem to be excessive to demand that Daniel wait for another person to arrive on the scene before looking for the dead person's wallet.

The second case involves a spouse who is suspicious that his partner is having an affair. To this end he starts to read his spouse's e-mail and check her text messages when she is asleep in order to discover the truth. While it may be better for him to declare his intentions to a friend (acting in this case as a higher authority) it once more seems excessive to *require* this of him. Provided the other necessary conditions of surveillance are met there is no requirement that a declaration be made.

I therefore hold that such a declaration is a *pro tanto*, rather than a necessary, condition. The making of a declaration adds weight to a consideration of overall justification as it has some force insofar as the gaining of accountability is concerned (as well as other benefits attending declarations made to the surveilled subject). However, as I have shown, it would be excessive to demand that such a declaration be made of necessity.

8.6 Conclusion

I have argued that a declaration of surveillance is a *pro tanto* condition for just surveillance. Such a declaration can be made either to a higher authority or to the surveilled subject, or both. The benefits of such a declaration are that it brings with it an element of accountability to the surveillant in both cases. In the case of declarations made to the surveilled subject, the declaration can also bring about a change in behaviour and a degree of consent to the surveillance. However, there are cases in which no declaration needs to be made (although it would still be beneficial if it *were* to be made) and so it is not a necessary condition of just surveillance.

9. Chance of Success

The likelihood of success has long been seen as an important element in the just war tradition, governing whether a state is justified in declaring war. It has typically been thought that without a chance of success the war would be unjustified. I argue in this chapter that, as with war, the chance of success is a morally relevant criterion in considering surveillance. First I look at defining success. This includes what is meant by success, degrees of success, probabilities of success, and the costs against which success needs to be measured. From there I consider false positives and false negatives, in particular looking at how these are sometimes misapplied in suggesting the failure of a system of surveillance. Finally, I apply these considerations to a surveillance programme known as SPOT (Screening Passengers by Observation Techniques) and practiced in some US airports. SPOT received heavy criticism in 2010 when it transpired that it had not apprehended any terrorists and had allowed several known terrorists to pass through airports unmolested. In the light of my analysis concerning what is meant by success I shall argue that at least some of this criticism levelled at SPOT was unjustified.

9.1 Defining Success

I argue in this section that there are a number of criteria underlying the chance of success principle. These criteria are a justified cause against which success can be measured, the degrees in which success can come, the probability of success of a surveillance operation, and the costs attendant on that success. I look at each of these in turn below.

9.1.1 Justified Cause and Success

I argued in chapter 4 that there are a limited number of justified causes for non-consenting surveillance of mentally competent, autonomous adults, namely those stemming from liability and those in which the benefits significantly outweigh the costs. Given the reason for the surveillance occurring, it follows that the success of the surveillance should be measured in terms of how far it is able to achieve this end. Any condition of success thus requires there to be a clear justified cause.

That this is the case can be illustrated by considering the alternative. Imagine surveillance had been put in place to identify and apprehend a rapist, and nothing else. If it fails to identify the rapist then it has not been a success. If there is no chance of it identifying the rapist then there is no chance of it being a success. This picture is complicated by the fact that there can be several justified causes for surveillance being used. A CCTV system in a supermarket may be put in place to identify shoplifters and lost children. It is plausible that it may succeed in one of these areas but not the other.

There are at least two problems which can arise from referring the chance of success to the justified cause. The first of these is when the measure of success starts with the justified cause, but then moves to encompass other ends not included in the original justifying cause. This is known as function creep. The second problem is when a specific justified cause is not known but there are suspicions that there might be one, if only enough data is examined. This is used to justify collecting large amounts of data without justified grounds for treating the people whose information is collected as liable. This collection is known as engaging in a fishing trip. I examine each of these below.

9.1.1.1 Function Creep

It is important that the justified cause be clear. If it is not clear then there may be scope for the justified cause to change from one that has been sanctioned to one that has not. This shift in purpose is known as function creep. Function creep occurs when technology is gradually applied to new ends or in novel contexts for which it was not specifically designed (Winner 1977 pp. 88–100).

Imagine that a CCTV system is put in place in a supermarket purely to identify shoplifters, but it transpires with time that it is also effective at identifying lost children. In this case there is a shift in purpose from one just cause (identifying shoplifters) to another just cause (identifying lost children). Here both of these causes carry weight in terms of justifying the surveillance. However, the stated cause should carry greater significance in terms of justification. If it turns out that the CCTV system is terrible at identifying shoplifters (despite that being its stated purpose) but excellent at identifying lost children, then its stated just cause should change from being the identification of shoplifters to being the identification of lost children. In the absence of this change there is a risk that the system's

success will be measured against the wrong criterion. There is also an attendant danger that without this change the system will be used primarily to identify shoplifters and in the process fail to identify as many lost children as might otherwise be the case. It will hence be less effective in achieving the main justifying cause than it might be.

On the other hand it may be that the system is good at identifying shoplifters *and* children. If this is the case then the operator may find himself torn between watching people whom he suspects will steal from the shop, and watching children who appear to be about to wander off from their parents. In this case the increase in functions causes the operator to dilute his efforts and risks the system being less successful in its stated aim of identifying shoplifters.

The function creep from identifying shoplifters to identifying children is one possibility involving a shift from one justified cause to another. There is also the possibility that function creep might involve a move from a justified cause to one that is not justified. For example, the same CCTV system is found to be effective at looking down the blouses of women reaching into freezers in the supermarket. As before, it might transpire that the system is not very effective at identifying shoplifters, but very good for looking down women's blouses. In this case it is *only* the justified cause that can carry any weight in assessing the success of the system. The fact that the system is successful in achieving a cause which, I will assume, is not justified is irrelevant in terms of morally assessing the success of that system.

There are hence at least two concerns with function creep. Firstly, there is a concern that the system may not be as effective at achieving the justifying cause as it might be, if it is not clear that the justifying cause has changed. Secondly, that technology with a specific and legitimate use in one context is applied to increasingly broader contexts. As this happens, the aspects of the technology which made it an initial success may be diluted. A third concern is that the technology and content, such as personal data, collected for one purpose (e.g. health records) can migrate to fulfil other functions. These functions extend the technology, its uses and its costs beyond "what was originally understood and considered socially, ethically and legally acceptable" (Ball et al. 2006 p. 9).

The problems with function creep discussed above may invoke a slippery slope argument. As the operator's attention is divided, so the system becomes less effective at meeting its justifying objective. Alternatively, as the purposes of the surveillance multiply, so there is a risk that they will cross over from the acceptable to the unacceptable without sufficient accountability. These are not logical slippery slope arguments (there is no necessity that the slippery slope occurs) but rather they are empirical/psychological. That is, given past experience and a broad understanding of human nature, the envisaged risk is plausible or even likely to occur (Glover 1990 pp. 166–67; Grovier 1982). Along these lines, it is important that the purpose (the justified cause) of the surveillance system is clear. The more obscure the purpose of a system, the easier it is for the system to encompass objectives not initially sanctioned.

That this is the case can be seen in the study of the implementation of CCTV in the UK by Martin Gill and Angela Spriggs. The study found that "many projects did not have clear objectives. Partly this reflected an uncritical view that CCTV was 'a good thing' and that specific objectives were unnecessary" (Gill and Spriggs 2005, x). All of the systems they considered "had the overall *objective* of reducing crime [emphasis added]" (Gill & Spriggs 2005 p. 22) as well as reassuring the public and deterring offenders, but the *evaluation* of these systems included finding missing children and attracting funding (Gill & Spriggs 2005 p. 117).

This is not to suggest that it is bad to find missing children or attract funding. In this case the justified cause seems to have expanded from reducing crime to finding missing children. As noted, this could lead to a change in or dilution of the stated justified cause such that the system is not as effective as it might be. It may also allow for further broadening of the criteria for success to include purposes which would not be just causes. This is a particular concern if there is no scope for accountability and transparency of the authority conducting the surveillance. Without such transparency there is a danger that the adaptation of purpose can occur subtly in a piecemeal fashion over time and so bypass much-needed ethical oversight.

9.1.1.2 Fishing Trips

A further area of success which invokes the need for a justified cause is so-called "fishing trips". These occur when a target, who is suspected of having information which may be of interest to the surveillant, is put under surveillance "just in case". The phrase "fishing trip" likens to surveillance to dragnet fishing in which a wide net is pulled through the water to catch a large number of fish indiscriminately. In a similar way surveillance is applied to people's lives to uncover information which it is believed will justify the surveillance *post hoc* (or, more cynically, if not justify then at least sell newspapers if the surveillant happens to be a journalist).

The justification of fishing trips can be determined, at least in part, by reference to the justified cause. Does the subject consent to the surveillance? Presumably not. Will the surveillance lead to significant benefits and minimal harms? In this case it is not clear how the harms of fishing trips are minimized, nor that the benefit would be significant. In that case the surveillant must have reasonable evidence that the surveilled subject can be treated as liable.

If, for example, the security services have reasonable evidence that Fred is planning to blow up an aircraft as an act of anti-capitalism protest, it may be justified for those services to monitor Fred. This surveillance can be to find out more about the plan itself, but also to see whether more information about Fred's partners in crime and other plans Fred might have can be uncovered. If, though, the security services do not have reasonable evidence that Fred is planning to blow up an aircraft, nor any to suggest any past action of sufficient gravity which the surveillance could help to address, then such surveillance would be unjustified.

By the same token, if an investigative journalist has reasonable evidence that a politician is engaged in some wrongdoing of sufficient gravity then surveillance of some sort may be justified. If, on the other hand, the journalist merely suspects that he will find a story if he hacks into that politician's voicemail messages, then this is clearly unjustified. In both cases (the security services and the journalist) it is important to note that while the absence of a justified cause renders surveillance unjustified, the presence of such a cause does not

alone justify the surveillance. The other principles of just surveillance (proportionality, intention, declaration of intent, etc.) must also be met.

In both of these cases, though, the acceptable instances of surveillance are not fishing trips. They occur on the basis of reasonable evidence of liability. Fishing trips, on the other hand, occur on the basis of possible information of interest to the surveillant. That is, in the above cases, the fishing trips are those which I have described as unjustified. Fishing trips therefore cannot be justified as they fail to meet the criteria for a just cause.

9.1.2 Degrees of Success

When can an act of surveillance be deemed successful? I have suggested that success lies in achieving the purpose of the justifying cause(s). However, this is not as straightforward as it may at first sound. Success could be taken to infer a binary outcome: success or not-success. That is, either the objective of the justifying cause was met or it was not. This is of course logically true, yet it is not the case that not-success is (necessarily) tantamount to failure. Not-success, taken as not meeting the objective in its fullness, is not necessarily the same as an overall failure of a surveillance system or operation, although it might be.

Success can come in degrees. An operation does not *have* to meet 100% of its objectives in order to be successful. Indeed, it may be impossible, or implausible, for such an operation to meet 100% of its objectives, and yet the operation still plausibly be a success.

The degree of success involves two criteria: the significance of the success and the numbers involved. In a simple surveillance operation, such as the police staking out a serial killer, these variables are comparatively straightforward. The significance is encapsulated in apprehending a serial killer, the harm of whose actions is great and affects a number of people, and the number involved is one (the rapist). The victims on whom the serial killer would prey before his eventual capture form a part of the first criterion (significance). For example, the apprehension of any murderer is significant, but it is surely more significant to catch a serial killer who is likely to carry out more attacks, than to catch someone who murdered one person and, for medical reasons such as developing locked-in syndrome, is then unable to kill again. Obviously there is a subjective element in this as well. The significance of the apprehension of the murderer will be greater to the families of his

victims than to others with no connection to the case. However, the objective significance of the apprehension is tied to the number affected in the past and likely to be affected in the future.

Alternatively, we might imagine an airport surveillance system. For the sake of the argument I will posit that this system exists only for security and not for monitoring traffic flow or other possible ends. As such, the justified cause for the system is the security of the people using the airport, but how is this measured? Preventing a terrorist from boarding a plane that he intends to blow up meets the criteria well. The significance of the success (preventing a plane full of passengers being destroyed) is substantial, and the numbers involved low.

Yet airport security systems do not often catch terrorists. It may be that the system exists to deter terrorists, in which case success would be measured differently, i.e. in terms of number of terrorists deterred and the significance of their terrorism. More frequently, airport security systems catch petty criminals and those travelling with false papers, such as illegal aliens (Lord 2010 p. 44). In this case the significance of the success is moderate (by comparison with capturing a terrorist or rapist) but the numbers high (there are a large number apprehended, again by comparison with the terrorist or rapist). That is, there are more people apprehended as a result of the surveillance system monitoring moderate wrongdoings than there are in it monitoring graver wrongdoings.

9.1.3 Probabilities of Success

Success is rarely assured. That is why the principle in the just war tradition is described as *chance* of success. Going back to the airport security system, it may be that the system has a 1% chance of a significant success (i.e. apprehending a terrorist) and a 90% chance of a moderate success (i.e. apprehending illegal aliens). In neither case is success guaranteed.

If there is a low chance of success then it will be harder to justify the surveillance. However, it does not follow that a low chance of success should rule out the justification of an act of surveillance *in toto*. It may be that, while there is a low probability of success, *if* successful the surveillance will apprehend a significant wrongdoing.

For example, infiltrating a terrorist organisation with a single agent in the hopes of finding details of forthcoming operations may have a low chance of success, and a high chance of the agent being discovered and killed. Nonetheless, the possibility remains that a significant wrongdoing could be averted and a large number of people involved in that wrongdoing apprehended. If, on the other hand, there were no chance of the agent being successful then his life would be needlessly imperilled and this would be wrong.

Contrast the infiltration of a terrorist organisation with the infiltration of a group of graffiti artists. What they do in defacing property is wrong, but it is not as grave a wrongdoing as killing people through acts of terrorism. Presume that, like the terrorists, this group is particularly hostile to infiltrators and will kill them on discovery (but otherwise sticks to defacing property). Given the reduced significance of the wrongdoing of defacing property, it would require a higher probability of success to justify infiltrating the group at such a risk, if then.

9.1.4 Costs of Success

The risk to an agent infiltrating a group is a cost to the surveillance operation. Even if the agent is not identified and killed, he will suffer considerable stress during the operation. Cost is properly a consideration for proportionality, which balances the cost of surveillance against its benefits (cf. chapters 10 and 11). However, I raise it in this context as both success and failure come with costs attached.

Taking success first, there is an opportunity cost to the surveillance operation. The operation involves resources which may be deployed elsewhere, but for the existence of the operation. There are also ethical costs. People not liable to be subject to surveillance might be harmed by that surveillance if it is insufficiently discriminating (cf. chapter 12). The surveillance may form part of a security system such as SPOT (see below), which deliberately funnels people by identifying large numbers of mostly non-liable people for surveillance and then narrowing these down through progressive surveillance filters of increasing intrusiveness. It may also be that the very existence of the surveillance is sufficient to chill some people from engaging in legitimate activities for fear of being watched.

If those are some of the costs of success, what are the costs of failure? In failure the costs of success are retained but added to them are the costs of the wrongdoing the surveillance was intended to prevent or address.

Once more, though, it should be remembered that there is no straightforward success or failure binary option in surveillance. There are costs in successful surveillance which, *ceteris paribus*, mount as the surveillance is less successful. It may be, though, that a more costly surveillance will be more successful than a less costly alternative. Hence installing CCTV cameras in every room in people's houses will likely be more successful in curbing domestic abuse than CCTV cameras in the street. However, placing CCTV cameras in every room of people's houses is far more intrusive (costly) than placing them in the street. If curbing domestic abuse is the *sole* justification for the use of CCTV then this cost needs to be weighed against the benefits of success.

9.2 False Positives and False Negatives[12]

When surveillance is less than 100% successful, those lesser degrees of success (and ultimately failure) often come in the shape of false positives and false negatives. False positives in this context are people who capture the attention of the surveillant even though they have done nothing wrong. An example here would be an alarm placed at the exit to a shop in order to detect those leaving the shop without paying for an item. Each person who sets off the alarm, even though they had paid for all of the items they were carrying, would be a false positive. The system would incorrectly identify that person as a shoplifter. By contrast, if a person really were carrying an item for which they had not paid and walked passed the alarm without setting it off then that person would be a false negative. That is, the system would incorrectly register that person as a non-shoplifter (or, more correctly, it would fail to register that person as a shoplifter).

There is some ambiguity as to when something or someone becomes a false positive or a false negative. As with the just cause, so also the target needs to be clearly defined to all concerned. For example, an airport security system might target terrorists, but this needs

[12] The following is adapted from (Macnish 2012) and used with permission, licence number 3176401090089.

further clarification. Leaving aside the complexities of the definition of "terrorist", is the target:

1) terrorists about to destroy an aeroplane (specific terrorists - ST), or

2) just any terrorist who happens to be passing through the airport with no intention of destroying an aeroplane on this visit (any terrorists - AT), or

3) any and all terrorists using the airport (both ST and AT)?

If ST is the target (1) then any terrorist not about to destroy a plane (AT) would be a genuine negative for that system. It is not designed to uncover AT and so should not be judged on those grounds. While it may be bizarre, if the system is intended to identify just terrorists using the airport with no intention of destroying aircraft (2) then AT would be a genuine positive and ST a genuine negative for that system. If, though, the system is intended to identify any and all terrorists using the airport (3) then ST and AT would both be genuine positives.

While the target is defined simply as "terrorists", without clarifying whether "terrorist" refers to ST, AT, or both, this definition is ambiguous and open to misinterpretation. As such the definition of a false negative is relative to the aims and purposes of the system. This ambiguity, I shall argue, played a large part in the critique of SPOT as it was used at US airports.

9.2.1 False Positives

The definition of false positives, I have argued, relies on clear and unambiguous definitions of the target. If the security system is designed to locate AT and ST then any terrorist will be a target. If, on the other hand, it is designed to locate ST then any terrorist who is identified as a terrorist, even though he is flying to see his mother with no intention of an attack on this occasion, would be a false positive.

There is a further problem affecting false positives in that there are often stages of filtering before a final decision is made. Keeping with the airport security system we might say that a false positive is any innocent who is incorrectly imprisoned as a terrorist. I will call this a

final false positive. If, though, the stages of filtering are taken into consideration then there will be false positives at each stage. Indeed, the system might be designed specifically recognizing that there will be false positives, hence:

- Stage 1 – CCTV operators look for suspicious individuals;
- Stage 2 – CCTV operators take a sustained look at individuals passing Stage 1;
- Stage 3 – ground-based agents take a sustained look individuals passing Stage 2;
- Stage 4 – ground-based agents remove individuals passing Stage 3 for interview;
- Stage 5 – the arrest or release of any individuals passing Stage 4.
- Stage 6 – the trial and imprisonment/release of any individual passing Stage 5. This is the final stage.

In this system the successive filtering is designed to accommodate false positives, albeit fewer at each stage. Hence Stage 1 might involve 1,000 false positives, Stage 2 involve 500 false positives and so on until Stage 6 has relatively few false positives. Each of the stages prior to the final stage therefore has its own false positives, or non-final false positives. At each stage there is an increased cost on the innocent (the false positives), from increased monitoring to interview, arrest and even imprisonment. While the these costs to the innocent are obviously regrettable, they may be felt to be a price worth paying for the evil avoided. Alternatively it may be felt that at a certain stage the cost to the innocent becomes too high for the relative significance and number involved and the continuing probability of success.

A system, such as that described, might be designed to accommodate false positives at different stages to allow for progressive filtering. In a perfect system it would obviously be better that there be no false positives at all. An ideal system would apprehend all and only the guilty. However, such an ideal system is almost certainly not achievable. Nonetheless it may be tempting to think that if no false positives is the ideal, then fewer false positives is better than more.

This, though, is not necessarily the case. It is plausible that false positives prove to be beneficial. For example, the recognized existence of false positives in a partially-automated system can help to reduce operator complacency. By a partially-automated system I mean one in which a computer carries out initial scanning of unfolding scenarios

and then alerts the operator to suspicious circumstances, such as the leaving of an unattended bag. Should the operator believe that a partially-automated system functions effectively without him he may pay less attention to decisions suggested by the computer, even though the computer is not in fact totally reliable. The operator may therefore simply cease to notice threats not recognized by the computer, or he may authorise all suggestions as a matter of default, without checking them adequately. There is hence a risk of too much faith being placed in the computer by the operator. In this instance, allowing a greater number of non-final false positives to exist (assuming there will be some) might reduce the operator's temptation to rely on the computer. If it is known that 60% of the cases flagged up for his attention will be false positives then it might prevent his becoming too complacent. Hence in some cases a higher number of non-final false positives might not only be manageable but also preferable.

So far I have considered a case in which there is a just cause (the apprehension of terrorists) with, I have assumed, some probability of success (putting to one side for the moment the ambiguities as to whether the system is targeting ST, AT or both ST and AT). Of the many people using airports, few are likely to be terrorists, but I take it that the discovery and apprehension of even one terrorist is significant. Hence the significance of a successful surveillance operation would be high. What, though, of the cost of the surveillance?

Take first the cost to the subject under surveillance who turns out to be a false positive. In the above case Stages 1-3 impose comparatively little cost on the individual under surveillance. That he is identified as a potential target at Stage 1 and then dismissed as a false positive at Stage 3 might occur without his knowledge. This is not to say that such surveillance is cost free. The suspect may suffer from a violation of privacy or an unknown harm such as stigmatization as a result of the surveillance. However the cost incurred increases significantly at Stage 4, the interview, when the suspect is inconvenienced and is likely to feel harassed. This may be especially true if the suspect is a member of an identifiable group which receives regular attention, in which case the harassment may be accompanied by stigmatization. At this stage it is more costly to be incorrectly identified as a genuine target and hence the presence of false positives in the system becomes more problematic. Stages 5 and 6, arrest and imprisonment, are more costly still. As the cost increases, the significance of the success of the operation needs to be weighed against the

cost to the false positives. It is possible that success will prove to become too costly, and so the operation should not continue.

The question of costs cuts both ways. While there are costs to the surveilled subject there are also costs to the surveillant. Operationally, the greater the number of false positives, the greater will be the difficulty in finding the genuine cases. This is akin to finding the proverbial needle in a haystack, the false positives contributing to the amount of hay.[13] The number of *final* false positives may be mitigated by increasing the stages of filtering, but this is costly in terms of time and resources. Furthermore the later, more intrusive stages (i.e. those involving ground-based agents) are likely to be more resource-intensive. As such it would be preferable for the surveillant to reduce the number of non-final false positives before this stage, especially if that can be done with minimal cost to both surveilled subject and surveillant.

There is a final question which is the extent to which final false positives may ever be good. Here I have described final false positives in terms of the overall security system, of which a large part is surveillance. The final false positive in this system is therefore an innocent person being imprisoned as a terrorist. While this is an undoubtedly high cost on that person, there would be a competing high cost to society were that person genuinely a terrorist who was released. In the courtroom there is a position of uncertainty which the court attempts to resolve through appeals to certainty being "beyond reasonable doubt". It is apparent, though, that innocent people are sent to prison. However, if the alternative involves releasing terrorists then it may be felt by some that final false positives, while not good, are a price worth paying.

9.2.2 False Negatives

The notion of releasing a terrorist at the final stage raises the prospect of false negatives. It is possible to say that, to some extent, every false negative is a failure of a particular system. Each is an example of one who "got away". However, no system is perfect and so some false negatives are to be expected. There are, as I have said, degrees of success and so the existence of some false negatives does not equate to the complete failure of a system.

[13] I shall not deal here with the possible counter-example of "big data" as there is still scant evidence of the efficacy of such an approach at the time of writing.

Nonetheless we should aim to reduce the degree of error. The extent to which we should do this will once more depend on the cost of the false negative when weighed against the cost of the action which the surveillance is intended to address. If for instance the intended targets are terrorists about to blow up a plane then one false negative is much more significant than a person entering a country without valid travel documentation because he is seeking work as an illegal alien. This, though, should be weighed up against the fact that there are likely to be far more illegal aliens seeking transit than there are terrorists.

Given that there may be several security systems in place it is possible to distinguish between final and non-final false negatives in the same way as with false positives. If one is considering a single filtration system such as that described above (taken out of the context of the overall complex of systems in the airport) then every false negative is likely to be a final false negative. Once a person has been eliminated from that single system it is unlikely to spend any more time processing him as a potential threat. If considering a system in the context of an overall complex of systems (that is, every surveillance system in place in the airport rather than just the single filtration system), a non-final false negative is less problematic as the target may be located by a different system. He would only class as a final false negative if he passed through *every* system undetected.

Hence a terrorist may be recognized by the above filtration system, make it to Stage 3 and then be rejected from consideration before being called for an interview. The filtration system has failed to recognize him as a threat, and so from this perspective he is a false negative. However there will be other systems in place in the airport. It may be that he is identified at passport control, interviewed and arrested as a terrorist. In this case while he was a false negative to the filtration system, he was not a false negative to the overall system of airport security. Alternatively, it may be that he passes through all of the airport's security systems, boards the plane and blows it up. In this case he is a false negative to each of those security systems as well as to the overall system of airport security.

It is obviously better, within the logic of the surveillance system, for there to be fewer false negatives rather than more. The existence of false negatives implies that there is room for improvement in the system. As with false positives, it is likely that no system will ever be 100% effective, and so no system can guarantee an absence of false negatives. However,

unlike false positives it is hard to see where the known existence of false negatives could be a benefit, other than to highlight room for improvement and/or the need for a number of complementary systems, creating an overall complex such that false negatives are reduced.

9.2.3 Costs

False positives can contribute to harassment and stigmatization. False negatives indicate that the system is not perfect and could be improved upon. Furthermore, the cost of false positives and false negatives will increase as each subject progresses through the system. In the case of false positives in a filtration system as described above the costs increase as intervention becomes more intrusive. In the case of false negatives the potential cost increases the more security systems fail to recognize the threat. Ideally, then, a system will seek to reduce final false positives and final false negatives as much as possible. To do this, though, it may seek to increase non-final false positives provided they come at a relatively low cost.

I have argued that the toleration of some false positives might be beneficial to the system. This is especially true if those are low-cost non-final false positives. It would be preferable to have more rather than fewer low-cost non-final false positives if this proved necessary to avoid false negatives.

To illustrate this imagine the discovery that healthy suicidal terrorists about to destroy a plane almost always walk at 60m/min, while the majority of non-terrorists walk faster than this. Software could then be developed which targeted people walking at this pace. The operator could function, in theory at least, as a second filter to remove the false positives (non-terrorists walking at that pace) before ground-based staff intervene.[14] However there may be terrorists who limp owing to some prior carelessness in placing bombs and so walk at a slower pace. Rather than miss these limping terrorists it may be worth expanding the range of the software to recognize those walking at 60m/min and slower. This could expand the number of non-final false positives extensively, but the return (recognizing limping terrorists) might mean that the burden of the extra non-final false positives would be deemed worthwhile to avoid false negatives.

[14] Quite how the operator would do this in practice need not be of concern for the point at hand.

If this is true of non-final false positives, what of final false positives where the operator's decision is the final stage of the process. Once more this would depend on cost. For example, if the operator's authorisation led to a remote-controlled gun shooting the suspected terrorist there would be a much higher cost to false positives than if his authorisation informs a ground-based agent to interview the subject. In the latter case the stage is final from the perspective of the surveillance, although not from that of the overall process. In the former it is final from the perspective of both the surveillance and the overall process. In either case the impact of a final false positive is likely to be greater than that of a non-final false positive. As such, and while the core issue is still one of cost, it will likely be the case that final false positives should be reduced where possible.

9.2.4 SPOT

A helpful illustration here is the US Transport Security Administration's (TSA) Screening Passengers by Observation Techniques (SPOT) programme. SPOT operates at certain airports and involves the behavioural profiling of passengers, looking for "facial expressions, body language, and appearance that indicate the possibility that an individual is engaged in some form of deception and fears discovery" (Lord 2010 p. 10). Deploying 3,000 officers to 161 US airports, the TSA is estimated to have observed 2 billion people between May 2004 and August 2008. Of these, 151,943 were subject to secondary screening, 14,104 were then interviewed, and 1,083 were arrested (Lord 2010 p. 44; see also Mica 2010). During this period the US Government Audit Office (GAO) believes that "at least 16 of the individuals allegedly involved in [terrorist] plots moved through 8 different airports where the SPOT program had been implemented … on at least 23 different occasions" (Lord 2010 pp. 46–47). None of the sixteen were apprehended by officers involved with SPOT. Following the GAO report there was discussion in the media and by politicians over the "failure" of SPOT to apprehend a single terrorist (cf. Harwood 2010; Keteyian 2010). This, however, is a flawed response for a number of reasons.

The definition of false positives/negative depends as I have shown on the purpose of the system. The stated purpose of SPOT is to help identify "persons who may pose a potential security risk at TSA-regulated airports by focusing on behaviours and appearances that deviate from an established baseline, and that may be indicative of stress, fear, or deception" (Lord 2010 pp. 1–2). In particular, SPOT was intended to "deter terrorists" and

"counter terrorist activities" (Lord 2010 pp. 9, 29, 41). It did not limit itself to terrorism *per se*, though, and included criminals posing a risk as a target (Lord 2010 pp. 32, 35, 36, 58). Ignoring the complexities in the definition of "terrorist", a "potential security risk" could thus fall into one of four categories, three of which we have already encountered: a terrorist about to destroy a plane (ST), all terrorists not about to destroy a plane (AT), any and all terrorists (ST and AT), and non-terrorist criminals (NTC).

Given that it was a surveillance programme based on recognizing suspicious behaviour and leading to interviews, the final stage of SPOT should be considered those referred to interview. Final false positives would then be those referred to interview but not subsequently arrested. If SPOT had been intended to catch *just* ST and/or AT it therefore produced 14,104 final false positives, namely those referred to interview but not arrested for ST- or AT-related offences. Given that it was arguably intended to catch NTC as well, though, these arrests should count as genuine positives.[15] If so then the number of final false positives was 13,021, that being the number of people identified for interview and not arrested. This is noteworthy for it is at this stage that a significant cost was levied on both surveilled subject and surveillant in requiring an intervention and interview to take place. In terms of non-final false positives, i.e. those identified for secondary screening but not subsequently arrested, the number was 150,860.[16]

The SPOT programme therefore produced a large number of false positives, some bearing a higher cost than others. These were processed at a cost to both the TSA and those selected for interview, for comparatively little gain (1,083 arrests, none of which was for a terrorist-related offence). At the same time it is known to have missed 16 people who would be classed as AT. SPOT therefore does not recognize AT but it is successful in recognizing at least some NTC. However, uncovering AT by means of behaviour analysis alone would be ambitious to the point of fantasy. Through profiling behaviour there seems little reason why SPOT should locate any terrorist using the airport for innocent purposes (i.e. to visit their mothers). The alleged terrorists may not have evinced any suspicious behaviour and

[15] Given that 39% were illegal aliens, 19% had outstanding warrants and 16% were in possession of fraudulent or suspect documents, however, it is questionable as to how much of a threat these individuals posed to airports (Lord 2010 p. 44).

[16] An alternative calculation here would determine the false positives at this stage being those identified for secondary screening but not referred to interview (i.e. 138,922) *vice* those identified for secondary screening but not arrested.

so be undetectable by this method. It is therefore fallacious to judge SPOT against catching AT unless this was its purpose. However, the stated purpose was ambiguous and open to misinterpretation. Apprehending AT might therefore have been the purpose or it might not. If it was, then it was an unrealistic purpose. If not, then SPOT should have been clearer as to exactly what its purpose was. Either way, the ambiguity in its purpose seems to be at the heart of the criticism. By contrast, ST is a more realistic goal, but owing to the rarer circumstances of terrorists blowing up (*vice* travelling on) planes, it is harder to evaluate success against this criteria.

Throughout the analysis of the SPOT programme's success there is an interplay between the different criteria listed above. There was a just cause (the apprehending of security threats), although this was poorly stated, allowing for ambiguities in the judging of success. The threats of high significance (terrorists) were few and those of medium-to-low significance (illegal immigrants) were many. The probability of success, depending on the just cause, were reasonably high in the case of apprehending illegal immigrants (who are not trained to avoid acting suspiciously in airports), to low in the case of AT (who had no reason to act suspiciously in airports) and ST (who I shall assume are trained to avoid acting suspiciously in airports). The cost of success increased at each level of filtering. Initially false positives faced relatively low cost in terms of infractions of their privacy in a public place known to employ surveillance for security purposes. However, as they passed successive filters the false positives faced increasingly greater costs of intrusiveness, inconvenience, harassment and possibly also stigmatization.

Taking SPOT to concern ST, then, the cause was just, the significance high (but the numbers low), the probability high and the cost initially low but increasing to high. This seems to be a worthwhile pursuit, then, from the perspective of the chance of success. If SPOT were focussing on AT, though, while the cause was just and the significance high (but the numbers low), the probability was low and the cost initially low but increasing to high. This decreased chance of success makes the targeting of AT through SPOT in the face of the costs harder to justify. Finally, if the focus of SPOT were on NTC then the cause was just (I shall assume for argument's sake), the significance low (but the numbers high), the probability high and the cost low but increasing to high. In this case it must be asked whether the cost of SPOT was a price worth paying for the apprehending of NTC's

of low significance. In this way, the analysis of success outlined above can be seen to apply effectively to understand the success or otherwise of SPOT.

In conclusion, false positives and false negatives may lead to excessive costs being placed on a system or those it monitors. However, the number of false positives and false negatives will be determined in part by the purpose of the system. It is therefore important that this purpose be spelled out clearly and precisely. If SPOT had a fault, this was it. The wording of its purpose apparently allowed some to believe that it was a means of capturing any and all terrorists who flew from participating airports, no matter the reason for their travel.

9.3 Deterrence

There is a final point regarding deterrence. Security systems often attempt two functions: apprehension and deterrence. So far I have looked at apprehension insofar as the system is attempting to catch terrorists. The second function of a security system in airports is to deter would-be terrorists from attempting to stage an attack on or through an airport. SPOT, I have argued, was judged primarily and unfairly on the basis of the purported false positives and false negatives. SPOT was never publicly declared, and so did not, in and of itself, form a deterrent. However, it was a part of an officially-acknowledged increase in airport security in the US following the attacks of September 2001. Some of these increases were publicised and some were not. It therefore formed a part of an overarching programme of deterrence. There appeared to be no appreciation of this in the critiques levelled at SPOT mentioned above.

Deterrents such as this are very hard to judge from the perspective of success. How can the success of a deterrent be judged? Remaining with the example of an attack on an aircraft, it may be that an attack is planned but then abandoned owing to the high level of security. In this case the deterrent has been effective. However, it is unlikely that the abandonment of that plan will be known to any other than the terrorists involved. From the perspective of those involved in operating the deterrent the consequences are identical to those one would expect if there had been no such plan (i.e. no planes are destroyed). Even here, though, it may be that there is no such plan because there never was a plan, or because those who might form such a plan did not because of the security. Hence there are three possible

reasons for planes not being blown up in this scenario: firstly that there is no plan to destroy a plane, secondly that there is no plan to destroy a plane because of the security system, or thirdly that there is a plan to destroy a plane but it is abandoned because of the security system. In this scenario the deterrent can be said to be successful in the latter two cases and untried in the first case.

In contrast there may be a successful attack on an aircraft. Does it then follow that the deterrent has failed? Not necessarily. Certainly in this second scenario there was a plan which was executed, and so from that perspective the deterrent was not effective. However, there may have been other plans which were abandoned because of the deterrent. The deterrent may also have made it harder for terrorists to have carried out their plans, effectively reducing the pool of terrorists capable of blowing up aircraft. Hence even in the case where the action that the deterrent is intended to deter actually occurs, it does not follow that the deterrent is not a success.

It is hence not possible to assess the success or failure of a security system from the perspective of deterrence simply from the data available concerning the actions the deterrent was intended to deter. That is, if no planes were blown up it does not follow that the deterrent was successful, nor that it was unsuccessful (in whatever degree). More information is needed regarding which groups might have wanted to blow up aircraft and why they decided not to. Similarly, the fact that an aircraft was destroyed does not point to a (total) failure of the deterrent. Certainly it failed to deter that one act, but it may have successfully deterred tens or even hundreds of others. If this is the case then it is plausibly a very successful deterrent which should not be abandoned.

9.4 Conclusion

I have argued in this chapter that a surveillance operation's chance of success is a morally relevant criterion for consideration. The measure of success should be provided by the justified cause of an operation. However, this alone cannot meet this criterion. It needs to be accompanied by an appreciation of the degree of success, the probability of success, and the cost involved in the success.

There are, I argued, some problems in determining success. This I demonstrated through a consideration of false positives, false negatives, and the difficulties of establishing the success of deterrence. I finally turned to look at the case of the SPOT programme, active in some US airports, and at particular criticisms that have been levelled at this programme to the effect that it has been unsuccessful. Here I argued that these criticisms are either unfair or unfounded. They either assume a justified cause for SPOT which was never given (although the given justified cause was stated ambiguously) or that the justified cause for SPOT was vastly more ambitious than was realistic to expect.

10. Proportionality 1

In 2008 Poole borough council were suspicious that a family was falsely claiming residence in a particular school district in order to gain entrance to that school for their children. The school was a popular one and heavily oversubscribed. The council's response was to mount a 2-week surveillance operation involving following the family whenever they left the house and monitoring which lights were on at what times of the day and night. When it emerged that Poole district council had been engaged in this level of surveillance of one family, the response in the UK press was immediate and critical. In response, James Welch, of Liberty, said: "This is a disproportionate and unnecessarily intrusive use of [the Regulation of Investigatory Powers Act (2000)]" (Alleyne 2008).

The problems of disproportionate surveillance are not limited to Poole, though. A UK pressure group, Big Brother Watch, argued in 2011:

> Britain is unique in the widespread and relentless use of CCTV across every aspect of our lives. It continues to represent a disproportionate intrusion into the privacy of law abiding people, without delivering a corresponding improvement in public safety" (Pickles 2011).

In addition to examples of disproportionality, the importance of proportionality in ethical surveillance is recognised in law and academia. Regarding the UK government's legal abilities to intercept and retain communications data, Andrew Kernahan of the Internet Service Providers' Association has said, "It is important that proposals to update Government's capabilities … are proportionate" (Barrett 2012). Section 28 of the UK's Regulation of Investigatory Powers Act (RIPA 2000) stipulates that "a person shall not grant an authorisation for the carrying out of directed surveillance unless he believes … that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out." This is underlined in the *Code of Practice concerning Covert Surveillance and Property Interference* pursuant to the Regulation of Investigatory Powers Act, in which paragraph 3.6 states that the following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented (Home Office 2010)

Those in academia writing on the ethics of surveillance have also recognised the need for a principle of proportionality. David Lyon, John Kleinig, Gary Marx and Anita Allen all argue in its favour (Kleinig 2009; Allen 2008; Lyon 2001; Marx 1998). However, there is very little discussion in these writings as to what is meant by proportionality in the context of surveillance. In this chapter I address this lack, clarifying what is meant by proportionate surveillance and how proportionality should be determined.

Had the family in Poole been reasonably suspected of planning a major act of terrorism then the surveillance carried out on them would almost certainly have been proportionate. However, just as there are different degrees of wrongdoing, so there are differing degrees of response, surveillance being just one in a list of possible responses. There are also degrees of response within surveillance, a subject which will be taken up in chapter 11.

In this chapter I argue that proportionality is a necessary condition for ethical surveillance. I start by considering the analogy with proportionality in war. This is of course a key theme throughout the thesis and is no less helpful here than in other chapters. I then look at precisely what is meant by proportionality. In particular I examine which considerations should be weighed in the balance when deciding whether a particular course of action is proportionate. Here I draw particularly on the work regarding proportionality in war carried out by Thomas Hurka (Hurka 2005) and apply this to surveillance. Finally I consider some of the problems in achieving a considered solution as to whether an act is proportionate. My conclusion is that while the application of proportionality is not straightforward it is nonetheless a necessary factor in establishing the justifiability of surveillance.

10.1 Proportionality in War and Surveillance

There are generally taken to be at least two aspects of proportionality in war: the proportionality of declaring war (*jus ad bellum*) and the proportionality of particular acts of war (*jus in bello*). Hence the war itself may be a proportionate response to the occasioning cause, but a particular act may be disproportionate in terms of a particular battle. For example, using of short-range nuclear weapons in response to an enemy which had run out of ammunition for their guns and had no other weapons. At the same time, a war might be a disproportionate response to the occasioning cause (imagine a farmer extending his field across an international border. As a result the state into which he has encroached declares war on his state) while individual acts of that war be entirely proportionate. Hence, while the war is a disproportionate response to the cause, individual battles fought in that war may be fought in a proportionate way. That is to say, if a war is disproportionate from the *ad bellum* perspective, it does not follow that all acts of that war will be disproportionate from the *in bello* perspective. The proportionality of the individual act will depend upon the circumstances of that act rather than on the proportionality of the overall war.

Maintaining the analogy between the ethics of war and the ethics of surveillance would hence suggest that there also be two aspects of proportionality in surveillance. The first would be that of the decision to employ surveillance *per se*. This would be proportionality as a consideration of *jus ad speculandum*. The second concerns the method of surveillance being used, which would be an issue for *jus in speculando*, the oversight of means used to effect surveillance. Hence in the above quote by Big Brother Watch, the focus was not on whether surveillance as such would be disproportionate, but on CCTV in particular. That is not to say that Big Brother Watch does not see other government surveillance in the UK as being disproportionate, but in the quote the accusation of disproportionality is clearly addressed at the use of CCTV cameras in particular.

A possible objection here is that there is an important disanalogy between war and surveillance. War is of necessity harmful: people die and are injured in war. If nobody dies or is injured then it is arguably not a war. By contrast there are no necessary harms in surveillance *per se*. Certainly there are harms associated with surveillance (see chapter 3) and these harms are likely in most cases. Nonetheless, it is at least possible to conceive of acts of surveillance in which there is no harm (Doyle 2009). This being the case it may

make sense to talk about the proportionality of an *act* of surveillance but not of surveillance *per se*. Hence, in war, the harms are actual whereas in surveillance they are only potential. Thus, when considering proportionality in war, there is always a minimal necessary harm (death and injury), whereas in surveillance there is no such minimal necessary harm. This would allow one to take an optimistic view of engaging in surveillance such that there might be no harm at all in a particular case, thus rendering it proportionate.

Granted that there are minimal necessary harms in war and not in surveillance, this does not diminish the importance of the consideration of proportionality in the latter. It is possible to imagine a relatively harmless war in which only one person dies as a result of fighting before a truce is declared. If, in determining proportionality in going to war, a *best* possible scenario were considered then such a war would frequently be considered proportionate. By contrast a *worst* possible scenario could be envisioned (e.g. nuclear Armageddon wiping out the human race) and the war therefore always be considered disproportionate. Rather, in determining proportionality it should be the *plausible* or *likely* scenarios that are envisioned.

Such a consideration of likely scenarios must invariably include considerations as to the form the warfare is likely to take and hence involve some consideration of means (for example, whether the war will plausibly involve nuclear weapons or remain conventional). Likewise, a consideration as to whether to employ surveillance must include the likely forms that surveillance will take.

Does this conflate the traditional *jus ad bellum* and *jus in bello* principles of proportionality? I do not think so, although it may bring them closer together than is often taken to be the case. There is still a relevant distinction between a consideration at the outset of war as to what are the likely forms of warfare to be used and the consideration during the war of the most appropriate forms of warfare to be used at any particular time. Clearly these might diverge given the circumstances of the war. For example, an enemy thought at the outset of war to have purely conventional forces may turn out to have and use battlefield nuclear weapons, thus escalating the war beyond the level it was reasonable to predict at the point of declaration.

The same distinction between the plausible nature of the operation at its outset and the particular acts involved as the operation progresses is true of surveillance. The *jus ad speculandum* decision to employ surveillance must take into consideration the forms of surveillance likely to be used. This is distinct, though, from later decisions made once the surveillance is underway (i.e. at the *jus in speculando* stage) as to which forms of surveillance are most appropriate under the circumstances.

In this chapter and the next I address proportionality as it concerns surveillance in general (*jus ad speculandum*) and as it deals with methods of surveillance (*jus in speculando*). In the remainder of this chapter I concentrate on the philosophical issues surrounding proportionality in general, applying those issues to proportionate surveillance (*ad speculandum*). Chapter 11 will then focus on the methods of surveillance and attempt to understand the benefits and harms associated with different methods of surveillance (*in speculando*).

10.2 What Is Proportionality?

Proportionality is a term often used but rarely described. On the face of it, a reasonable starting definition would be that it involves the harms of a particular act not outweighing the goods of that act. I shall consider precisely what is meant by the terms "goods", "harms", and "outweighing" below, but for now it is sufficient to note that if the harms arising from an act outweigh the goods then that act is likely to be disproportionate. As it stands, though, this definition is in danger of committing to a consequentialist approach, which I rejected in chapter 1. I shall develop this understanding of proportionality below such that, while it does consider consequences, it is not a purely consequentialist consideration. In particular, I argue that not all benefits should count in favour of an act of surveillance and I argue that the difference between benefits and harms in favour of benefits should be significant, rather than slight, in order to render an act proportionate.

Originally used by Euclid as a mathematical term relating to relationships between shapes, proportionality is also used in ethics, particularly the ethics of war and of jurisprudence. However, while it is relatively easy to judge the proportionality existing between two objects such that one is twice the height, width and depth of the other (for example), it is less straightforward to judge the proportionality of human actions. When, for instance, is

an act of war proportionate, or the sentencing of a criminal disproportionate? Mathematical objects can be measured with a degree of accuracy and then compared. Human actions, by contrast, do not lend themselves to accurate measurement and so comparison is more difficult. There are a number of objections which arise from the application of proportionality to these ethical issues to which I will now turn. I will argue that each of these objections should be dismissed.

10.2.1 No Inhibitory Effects

The lack of a mathematical rigour that can be applied to proportionality as it concerns ethics has led to some questioning its usefulness. Michael Walzer, for instance, seems to dismiss the notion of proportionality in war, concluding that "the proportionality rule often has no inhibitory effects at all. Even if a large number of civilians lived in those five square miles near St. Lô, and even if all of them were likely to die, it would seem a small price to pay for a breakout that might well signal the end of the war" (Walzer 2006a p. 318). However, this case does not make the argument that Walzer seeks. If the deaths of a large number of innocents really *is* a small price to pay for ending a war then those deaths would be proportionate. In this case the proportionality principle should not be inhibitory. By contrast, if this case is *not* a small price to pay then it would be disproportionate and so would, or at least should, have an inhibitory effect. If, for example, three quarters of a country's population had to be annihilated in order to end a war over a farmer extending one of his fields into a neighbouring country then these deaths would be disproportionate and thus the principle would be inhibitory.

An argument similar to Walzer's would be to say that while the principle of "do not murder" is uncontroversial, it too does not have an inhibitory effect on murderers. However, even if people did not accept the principle of "do not murder", and so committed murder, this would not undermine the value of the ethical position. Rather the principle would serve to demonstrate that the murderer was wrong in committing murder. Furthermore, while it may not have an inhibitory effect on actual murderers, it may well do on potential murderers. If murder were not seen to be wrong then there would likely be many more murders. Hence a lack of inhibitory effect in practice should not lead to rejection of an ethical principle.

10.2.2 Political Re-description

A second challenge which may be levelled at attempts to use proportionality in surveillance, or indeed in any area of ethics, is the political malleability of the term. For example, one side in a conflict might choose to frame a particular action in the light of situation X, rendering that action proportionate. At the same time, the opposing side could frame it in light of situation Y (both X and Y being true states of affairs) such that the same act is not proportionate.

It is true that an act can be re-described in different ways, leading to potential confusion. However, this is arguably true of most moral teaching. Rape is wrong, but not consensual sex. The rapist may in retrospect genuinely see himself as having engaged in consensual sex, and so justified. However the act is described, though, and granting that there are limitations as to what a person not present can know, there is nonetheless a truth in the matter. Either the sex was consensual or it was not. Certainly there can be degrees of consent, and what is consented to. Returning to the above case, a consideration of proportionality would therefore need to take into account both X and Y.

10.2.3 Elasticity of Proportionality

A third concern regarding proportionality is what Oliver O'Donovan refers to as the elasticity of proportionality (O'Donovan 2003 p. 62). This is partly an epistemic problem of knowing when an act is proportionate or not and partly an ontological problem as to whether there even is a dividing line.

O'Donovan argues that this elasticity, whether epistemic or ontological, is not infinite, though. There are acts, he claims, which are clearly disproportionate, "which would be inappropriate to meeting any threat whatever. To be convinced of this, we do not have to determine precisely where the line of categorical disproportion is to be drawn; we only have to identify some case that lies beyond it" (O'Donovan 2003 p. 62). To employ an analogy O'Donovan uses of discrimination, we may say that, "while we puzzle over the twilight cases, we cannot overlook the difference between day and night" (O'Donovan 2003 p. 38). I shall consider this concern of determining proportionality in greater detail below.

Proportionality is therefore not an easy concept to apply, but it does not thereby follow that it cannot or should not be applied. While the point of reference may vary and while there may be elasticity in considerations of proportionality there remain acts which are clearly disproportionate and those which are clearly proportionate. Massacres such as that of the Polish officers at Katyn would be one such case in which the gains achieved (the elimination of those with presumed anti-Soviet beliefs in the wake of the division of Poland in the Molotov-Ribbentrop Pact of 1939) in no way merits the harms visited (the murder of thousands) (Stewart 2010; Fischer 2007). While the realm of surveillance does not include atrocities on the level of Katyn, the fictional case of total surveillance presented by George Orwell in *1984* (Orwell 2004) is a clearly disproportionate act that serves as a case which lies beyond the acceptable. By contrast, the Nazi-Soviet tank battle of Kursk in 1943 was a major engagement between two warring parties, each of which believed they had a good chance of success and from which each stood to benefit. This seems to be a proportionate act of war. In the same way, police monitoring the communications and movements of a gangland boss suspected of ordering a number of murders seems to be a proportionate act of surveillance.

10.3 Measuring Proportionality

I have argued that there are obvious and significant differences between the mathematical notion of proportionality and the ethical. One such difference is the ability to measure the act in order to judge it as proportionate or not. Perhaps even more problematic than this, though, is the question as to *what* is to be measured. In comparing plane shapes such as two squares there are two dimensions, height and width. In discussing an act with regard to its harms and benefits it must first be decided which harms and which benefits (as well as whose harms and benefits) are to be applied.

Writing in the context of war, Thomas Hurka has presented an excellent article on the concerns of proportionality which focuses clearly on the issues of which benefits and harms should be weighed in the balance (Hurka 2005). I argue below that Hurka's analysis of proportionality is a clear case in which writings in the ethics of war can be employed in resolving issues in the ethics of surveillance. I will first describe Hurka's analysis and then apply it to surveillance.

10.3.1 Benefits

In response to the question of which benefits are to measured in proportionality, Hurka argues that "the relevant goods [in proportionality] are only those contained in the just causes" (Hurka 2005 p. 40). That is, only those goods present in the justifying causes should be counted. Other benefits which may arise but would not be sufficient to justify a declaration of war, even when taken together, should not count towards this measure. In making this claim, Hurka positions himself against a classically consequentialist position which would count *all* benefits and *all* harms in the balance before seeking the optimal outcome.

Hurka is keen to avoid the conclusions of a consequentialist argument which may lead to counter-intuitive and even repugnant conclusions (Hurka 2005 pp. 39–40). For a consequentialist, a small benefit for enough people can outweigh the deaths of a smaller number of people. Furthermore, the nature of this benefit is not limited and so could include human rights benefits, but may also include economic benefits, morale boosters or even entertainment. This may lead to conclusions such that if particular war benefits enough people by entertaining them then it is "worth" the cost of a limited number of deaths.

Hurka points out that World War II contributed tremendously towards reinvigorating the US economy in the wake of the Great Depression of the 1930s. However, he argues that it would be wrong to count this as a benefit of the war to be weighed against the millions killed in the fighting and associated harms brought about by the war. If economic reinvigoration did count, as it would in a simple consequentialist perspective, then it would follow that it could be judged to be proportionate to wage war on a country for *purely* economic ends. Yet, as Hurka responds, "killing cannot be justified by merely economic goods, and the same is true of many other goods" (Hurka 2005 p. 40). He argues that, as the reinvigoration of its economy would not have been justification for the US entering the war, nor should it be counted as a benefit to be included in the balance when weighing up whether or not to go to war. I shall refer to the reinvigoration of a country's economy, along with similar benefits of war which should not count in the proportionality consideration (such as technological progress or meeting the desires of soldiers who are bored with training and want to go to war) as "peripheral benefits". That is, they are

benefits but they are peripheral to the considerations as to what should be counted in the balance of proportionality.

There are hence, according to Hurka, benefits which should count in determining proportionality and benefits which should not. The former, Hurka identifies as those "contained in the just causes" while the latter are what I have called peripheral benefits. It is important to note that Hurka recognizes two types of just cause. One is the sufficient just cause, those causes which "suffice by themselves to fulfil the just cause condition" (Hurka 2005 p. 41). The other is the contributing just cause. Of the latter, Hurka writes, "contributing just causes do not suffice to satisfy the just cause condition; given only these causes, one is not permitted to fight. But once there is a sufficient just cause, contributing causes can be further legitimate aims in war and can contribute to its justification" (Hurka 2005 p. 41). The difference between sufficient just cause, contributing just cause and peripheral benefits can be seen in Table 4.

Causes	**Benefits Relevant to Cause**	**Benefits Relevant to Proportionality**
Sufficient Just Cause	Relevant (sufficient)	Relevant
Contributing Just Cause	Relevant (contributory)	Relevant
Peripheral Benefit	Not relevant	Not relevant

Table 4: Benefits of Surveillance as they relate to Cause and Proportionality

As an example of contributing just causes, Hurka looks at the good of improving women's rights in Afghanistan, which he considers to be a benefit of the war which started there in 2001 to overthrow the Taleban regime. He believes that such improvements are also clear benefits to be had from the war, but unlike peripheral benefits he argues that these should be included in considerations of proportionality. However, as noted, these alone are not sufficiently strong reasons to go to war in the first place (Hurka 2005 p. 42). They therefore fall between goods which arise from those legitimating the war (part of the just cause) and which should be counted in the balance of proportionality, and peripheral benefits which do not legitimate the war and should not be counted in the balance of proportionality. Rather, these contributing causes do not legitimate the war but should be counted in the balance of proportionality.

There are hence three categories in Hurka's account: sufficient just causes, contributing just causes and what I have called peripheral benefits. Of these, justified causes are alone sufficient to go to war over. Contributing causes are not sufficient to go to war over, but may lend weight to the justified causes in the declaration of war. Peripheral benefits are not sufficient to go to war over and may not lend weight to the justified causes in the declaration of war. When it comes to weighing proportionality, both the justified causes and the contributing causes contribute to the benefits of a war. Peripheral benefits do not contribute to the benefits of the war *insofar as these are relevant to the proportionality consideration.*

Hurka raises the question as to whether there is a unifying feature to contributing just causes which gives them their status. His conclusion is that, "there is not; like the sufficient just causes, they are just the items on a list" (Hurka 2005 p. 43). However, he does acknowledge that there are "intuitive limits" to what can go on that list. If Hurka is correct in this, and I can think of no unifying cause that has eluded Hurka, then contributing just causes need to be dealt with on a case-by-case basis.

There are hence three categories of benefit which should be considered in the balance when weighing proportionality: those contained in the sufficient just causes, those contained in the contributing just causes, and peripheral benefits. Of these, the first two may be counted in the balance of proportionality as benefits, but the third may not.

This has taken the discussion a long way from considerations of surveillance, but it is not hard to see the parallel. In weighing up surveillance as an option, only certain benefits of surveillance should be included in the balance. Those benefits which serve as sufficient justifying causes and contributing just causes of the surveillance should be counted in the balance. Peripheral benefits should not count in this way. Hence, if we return to the case of Poole Borough Council raised in the introduction, the benefits which could be counted in the balance towards proportionality are the sufficient just cause (presumably detecting parents who are attempting to cheat the system of allocating school places) and any contributing just causes (such as protecting other parents from having their place in the queue to get their child into school "trumped" by a parent who can afford to move house, deterring other parents from attempting to cheat the system, etc). What should not count in

the proportionality balance are peripheral benefits, such as the employment of staff engaged in the surveillance.

The alternative, more consequentialist position would be to count *all* the benefits of surveillance in the balance. This would, for example, include the enjoyment which the surveillant received from the surveillance. It would then be feasible, given enough pleasure on the part of the surveillant, that his voyeuristic pleasure could outweigh the harms visited upon the surveilled subject by the surveillance. This would render the surveillance proportionate and, in those terms at least, permissible. Yet this conclusion is, I hold, ethically unacceptable.

10.3.2 Harms

Moving from benefits to harms, Hurka believes that there is "no restriction on their content parallel to the one on relevant goods" (Hurka 2005 p. 45). Hence all harms should be considered in the balance against the benefits, no matter how remote from the action (Hurka 2005 p. 46). He raises the interesting question of Kamikaze pilots used by Japan in WWII, pilots who were forced to kill themselves in order to inflict the greatest damage possible. In declaring war on Japan, should the US have weighed the cost of the lives of these pilots (who might have lived had their military endorsed different tactics) as harms? Hurka believes so, but with diminished weighting. Once more this translates easily into considerations of proportionality in surveillance such that all harms, no matter how remote from the action, should be taken into consideration when determining whether or not to take that action.

10.4 Balancing Harms and Benefits

The final consideration of this chapter in looking at proportionality insofar as it affects *jus ad speculandum* is that of how the harms and benefits are to be weighed. James Turner Johnson, for example, argues that the benefits must outweigh the harms in order for the proportionality condition to be met (J.T. Johnson 1999 pp. 27–28). An alternative position is put forward by Douglas Lackey, who expresses a concern that the interpretation described by Johnson is too restrictive as it will not permit many of the wars fought in defence of moral rights, as these may not lead to an overall benefit. However, he continues,

"according to most theories of rights, the maintenance and protection of rights is morally permissible unless the defence of rights causes *a great deal* more harm than good." By extension, Lackey holds that "a war for a just cause passes the test of proportionality unless it produces a *great deal* more harm than good" (Lackey 1988 pp. 40–41). Between Johnson and Lackey is a logical third position that the benefits should equal the harms in order for the war to be considered proportional.

Drawing on O'Donovan earlier in this chapter, I argued that there was a "twilight zone" between the obviously proportionate and the obviously disproportionate. This means that any call for equality between benefits and harms is unrealistic. This would require the precise measurements that I have argued are unavailable. As such, the third position suggested above of proportionality involving the equal balancing of harms and benefits is similarly unrealistic.

With the third position dispensed of, there remain two alternatives for balancing harms and benefits. Should one side with Johnson in requiring the benefits to outweigh the harms or with Lackey that the harms may outweigh the goods so long as there is not a great deal more harm than good? Johnson's position, as Lackey recognizes, tends to be restrictive while Lackey's is, by design, more permissive. Should one's default position therefore be with Lackey that war is generally proportionate unless the harms it occasions are *a great deal* worse than the goods it brings about, or should the default be with Johnson that war is generally disproportionate unless the goods it occasions are better than the harms it brings about?

Returning to the analogy of the twilight area, the issue is what to do with acts that fall within that area. Obviously acts to one side of the area ("clearly proportionate") are acceptable, and acts to the other side of the area ("clearly disproportionate") are unacceptable. The issue is what is to be done with (quite possibly the majority of) acts which fall within the area. Are they to be taken as proportionate or disproportionate?

There are three options in response to these questions. The default can be to presume proportionality unless there are strong arguments to the contrary. A second option is to presume disproportionality unless again there are strong arguments to the contrary. Thirdly, one could refuse to privilege one position over the other, on the basis that we

simply do not know which should be the default. Like W. D. Ross we could accept that, "our judgments about our actual duty in concrete situations have none of the certainty that attaches to our recognition of the general principles of duty" and make the best decision we can on a case-by-case basis (Ross 2002 p. 31).

While all three positions are tenable, I am disposed to come down in favour of a presumption of disproportionality in both war and surveillance. In both cases there are very real harms which are apparent and which the ethical framework is intended to guard against. It may be objected here that this is more plausible in war than surveillance, owing to the necessary harms of war. However, I have acknowledged, there are no necessary but merely likely harms in surveillance. Hence, the objection runs, there are better grounds for being more cautious in war than in surveillance. This objection overlooks the fact that here I am discussing that grey area in which it is unclear whether the harms are proportionate to the benefits. Where there are no harms, or the harms are genuinely minimal, then there is no question regarding the proportionality of the surveillance. Where there are harms, though, although not so many as to render the surveillance clearly disproportionate, I am advocating that one should proceed with caution. Those harms, as discussed in chapter 3, are significant. The more permissive approaches of Lackey and of deciding on a case-by-case basis leave open the possibility of those harms occurring which would otherwise be preventable. However, I accept that all three positions are controversial and merely comment that this is not intended to be the final word on the subject.

10.5 Proportionate Surveillance?

To return to the case of Poole Borough Council, I am now in a position to determine whether or not Mr Welch of Liberty was correct in his assertion that the surveillance was disproportionate. Presuming that the surveillance had a justified cause of attempting to detect parents cheating the school allocation system and deterring others from the same, these should count as benefits of the surveillance. The protection of other families who may be "trumped" by cheating families may, I suggested, be considered a contributing benefit. The employment of council staff in the surveillance was self-focused rather than other-focused and so a peripheral benefit, and as such should not count in the overall benefits in the proportionality calculus.

Against these should be weighed the harms of the surveillance. In Chapter 3 I posited that there is a number of potential harms. These include: privacy violations, vulnerability, fear of control, human error and abuse of power, and the fear of being "found out" when hiding legitimate but not criminal information. Of these, there was a privacy violation, a danger of error and abuse of information recovered, and a danger of legitimately-hidden information being recovered. Upon revelation of the surveillance there would also have been good grounds for the family to feel vulnerable. The likely alternatives to surveillance would have been at worst that a family "got away with it" in placing a child in a school to which that child was not entitled, or that a family continued in its legitimate business unmonitored.

From this analysis it does not seem that the council's act of surveillance was clearly proportionate. The benefits gained and the harms avoided seem to be comparatively small compared with the harms incurred by the surveillance. As such I agree with James Welch that the surveillance was disproportionate.

10.6 Conclusion

I have argued that proportionality is a morally relevant concern in surveillance, both in the decision to employ surveillance and in the methods used to engage in surveillance. This chapter has concentrated on the former of these, while Chapter 11 will deal with the latter.

Having provided a working definition of proportionality and raised some concerns with it, I drew on an article by Thomas Hurka to determine that only some benefits should be considered, whereas all harms should be weighed in the balance when determining proportionality. While no obvious unifying theory underpins what should be counted as a contributing just cause, I argued that none was necessary providing one was prepared to proceed on a case-by-case basis.

Finally, I looked at the problem of incommensurability of harms and benefits. In weighing proportionality I argued that one should default to an assumption that an act is disproportionate unless it is clearly proportionate. From this position I was able to return to the case of Poole Borough Council given in the introduction to argue that the surveillance carried out in the case in question was indeed disproportionate.

Proportionality is therefore a morally relevant consideration in the determination of whether an act of surveillance is ethical. It ensures that any harms which arise from surveillance must be balanced by the benefits stemming from the same surveillance. In this chapter, though, I have concentrated on the proportionality of employing surveillance. In the next chapter I will look at the proportionality of different types of surveillance.

Part III - *Jus in Speculando*

11. Proportionality 2

In October 2011, the Guardian newspaper ran a story concerning the Metropolitan police's use of a surveillance system. The opening sentence claimed that "Britain's largest police force is operating covert surveillance technology that can masquerade as a mobile phone network, transmitting a signal that allows authorities to shut off phones remotely, intercept communications and gather data about thousands of users in a targeted area … Barrister Jonathan Lennon, who specialises in cases involving covert intelligence and RIPA [the Regulation of Investigatory Powers Act (2000)], said the Met's use of the Datong surveillance system raised significant legislative questions about proportionality and intrusion into privacy. 'How can a device which invades any number of people's privacy be proportionate?' he said" (Gallagher & Syal 2011).

In response, "former detective superintendent Bob Helm, who had the authority to sign off RIPA requests for covert surveillance during 31 years of service with Lancashire Constabulary, said: 'It's all very well placed in terms of legislation … when you can and cannot do it. It's got to be legal and obviously proportionate and justified." (Gallagher & Syal 2011).

The language of proportionality is thus one that is recognized by both those employing surveillance, and those attempting to restrict that use, as an ethical limit. This should not be surprising. As seen in chapter 10, and referred to in the Guardian article, the need for surveillance by public bodies such as the police to be proportionate has been a part of British law since 2000. Furthermore, again as noted in that chapter, a number of academics writing in the field of surveillance ethics have similarly recognized the importance of proportionality.

In chapter 10 I looked at what proportionality is and how it should be resolved when deciding whether or not to use surveillance. That was under the consideration of *jus ad speculandum* – the justice of employing surveillance. In this chapter I look at proportionality as an aspect of *jus in speculando* – the justice of particular methods of surveillance. Hence whereas the former chapter focused on the *ends* which can legitimately be served by surveillance through linking proportionality with the just cause, this chapter focuses on the *means* of surveillance which can legitimately be employed for those ends.

That is, if the decision to use surveillance has been taken, the next question is which sort of surveillance should be used in which circumstances.

While it would be convenient to transplant wholesale the discussion from chapter 10 regarding proportionality, a cursory reflection will show that this is not possible. In weighing benefits and harms, I argued there that only certain benefits should be considered, namely those in the just cause (the sufficient just causes and the contributing just causes). However, the just cause is a specific feature of *jus ad speculandum*. While there is, as noted in chapter 10, some cross-over between *jus ad speculandum* and *jus in speculando* in the area of proportionality, this is not total. There is still an important distinction between the proportionality of surveillance as such and the proportionality of particular methods of surveillance. This chapter will therefore focus on the latter while drawing from chapter 10 where appropriate.

There are numerous types of surveillance which may be used in any one situation. CCTV; wiretapping; having people follow someone on car or by foot; loyalty cards; and keylogging are just a few examples. Clearly each situation could demand a different type of surveillance on pragmatic grounds. If the person to be placed under surveillance is known never to use a computer then keylogging is going to be of little use. However, more than merely pragmatic concerns should be taken into account when deciding which type of surveillance to employ. Each different type will involve introducing different harms, or different degrees of harm, on the surveilled subject. Furthermore, each method of surveillance (CCTV, wiretapping, keylogging, etc.) will involve different harms in different contexts. For example, CCTV in someone's bedroom could be more harmful than keylogging a computer in a call centre where there are strict rules prohibiting personal use of the computers, but keylogging an individual's home computer would be more harmful than CCTV in the street where that person usually shops.

In this chapter I consider the relevant harms and benefits attending particular methods of surveillance. Rather than attempt to produce an exhaustive list of each type and its respective harms and benefits (such a list would be cumbersome and quickly become outdated) I shall discuss the aspects of harm and benefit which are relevant to the proportionality consideration. For a more detailed discussion of plausible harms and benefits arising from surveillance, please refer to chapter 3. Consideration of the harms

will involve looking at the intrusiveness of the surveillance. In this I argue that the harms properly relevant to this principle are the harms occurring to the liable subject of surveillance, rather than to non-liable people. In the parlance of the just war tradition, this equates to harm visited on combatants rather than non-combatants. I also argue that there is an important distinction to be drawn between disproportionality as *excessive* behaviour and disproportionality as *inappropriate* behaviour. As in chapter 10, it is also important here to determine which benefits are appropriate to be weighed in the balance against the harms.

11.1 Definition

Proportionality involves, as I argued in chapter 10, a weighing of the benefits and harms associated with a particular act. In that chapter, discussing proportionality as an aspect of *jus ad speculandum*, I argued that only certain benefits should be weighed against all harms. I also argued that the benefits must outweigh the harms in order for the act to be proportionate. Insofar as a definition of proportionality is concerned, this is sufficient for this chapter.

Before considering which benefits and harms are to be weighed, though, I need to establish the relevance of proportionality to *jus in speculando*. The fact that it is relevant to *jus in speculandum*, as demonstrated above, does not mean that it is automatically relevant to *jus in speculando*. I provide the evidence of this in the next section.

11.2 Relevance

It may be argued that a person liable for surveillance is thereby liable for any and all surveillance. Short of supporting a draconian system of surveillance, this is obviously wrong. A suspected shoplifter may be liable for some surveillance but certainly not the same level of surveillance as a suspected terrorist. Even after surveillance has been established as an acceptable way of gathering information, the means that that surveillance takes is still an important moral consideration. It is possible that those means are either proportionate or disproportionate.

The idea that liable targets are still subject to considerations of proportionality sits at odds with some commentators in the just war tradition. These commentators, Thomas Hurka among them, hold that proportionality is not a proper consideration of combatant-on-

combatant fighting, but only of combatant-on-non-combatant fighting. This is equivalent to saying that proportionality is not a proper consideration of surveillance of the liable, but only surveillance of the non-liable. Hurka argues that "*in bello* proportionality as standardly understood seems to allow a nation to kill virtually any number of enemy soldiers to save just one of its own soldiers. Once a war has begun, enemy soldiers are essentially free targets that one may attack at any time. … If killing enemy soldiers now will prevent them from killing one of our soldiers in the future, it seems we may kill almost any number to achieve that end. … it seems we may kill virtually any number to save one of our soldiers" (Hurka 2005 p. 58). Hurka does not challenge this view, which strikes me, as noted, as being broadly akin to saying that there is no need for proportionality when confronting a legitimate target in surveillance.

If Hurka is correct in this then proportionality in a traditional understanding is employed in *jus in bello* only insofar as it concerns non-combatants. However, proportionality regarding acts which involve non-combatants is also a consideration of the doctrine of double effect. Within the context of the doctrine of double effect, the proportionality of acts against non-combatants makes sense. The targeting of non-combatants is, I argued in chapter 5, always impermissible. I consider the doctrine of double effect in greater depth in chapter 12. Briefly here it can be summarized as stating that targeting which would amount to the deaths of non-combatants is permissible if:

> a) the intention of the one engaged in targeting is not to target non-combatants;
>
> b) the number of non-combatants killed is proportionate to the end sought; and
>
> c) the killing of non-combatants would not be instrumental in achieving the intention of the one engaged in targeting,

To then take the *jus in bello* principle of proportionality as pertaining to non-combatants strikes me as undermining the principle of discrimination. The latter states that non-combatants cannot be targeted. However, the principle of proportionality, when taken to refer to non-combatants, seems to suggest that they *can* be targeted so long as the benefit is sufficiently great. This leads to a degree of inconsistency within the two major principles

of *jus in bello*: one treating the prohibition on targeting non-combatants as absolute, the other treating it as *pro tanto*.

A better approach is to see proportionality in *jus ad bellum* as concerning benefits and harms of the war *per se*; the proportionality principle in *jus in bello* as concerning benefits and harms insofar as they concern combatants; and the proportionality principle in the doctrine of double effect as concerning benefits and harms insofar as they concern non-combatants. This is certainly neater and avoids the inconsistency I have highlighted, but is it right? If Hurka is correct that, "we may kill virtually any number [of enemy combatants] to save one of our soldiers" then any discussion regarding the proportionality of combatant-on-combatant fighting would be largely irrelevant because almost any act would be proportionate.

I contend that Hurka is wrong in this. Imagine a contemporary colonial power bent on expanding its empire through military means. In its pursuit it encounters an indigenous people group who resist colonisation, sparking military engagement. Let us say that the indigenous group is armed with blowpipes and spears but the colonial power has all the materiel of a current dominant military. The soldiers of the colonial powers are equipped with clothing which makes them virtually invulnerable to enemy attacks, while they choose to deploy short-range nuclear missiles to massacre the enemy. This scenario is clearly disproportionate while involving only combatant-to-combatant fighting. Rather than "go nuclear", the colonial power could capture the enemy soldiers or use guns in a sufficient number of isolated incidents to persuade the enemy that they cannot win.

Now imagine that the indigenous people managed to capture a colonial soldier and hold him hostage. Does this change the situation? Is it now appropriate for the colonial military to deploy nuclear weapons in order to free him? I suspect not, at least while they have less severe options before them such as capturing a large number of indigenous soldiers and offering a swap. From this thought experiment I conclude that, contra Hurka, we may not kill virtually any number of enemy combatants to save one of our soldiers.

There appear to be two situations in which Hurka's description might be correct. The first is when the indigenous people have captured a colonial soldier and the *only* way to retrieve that soldier alive would be to kill a large number of indigenous soldiers. The second is

when by rescuing that soldier the war would be terminated. Of course, many would object that the colonial power should not be there in the first place. However, leaving that *jus ad bellum* issue to one side for the purpose of this illustration, it does seem as if there are situations in which Hurka is correct. These, though, are rare examples among many of combatant-on-combatant fighting, and should not be taken to be typical of other scenarios. Apart from such scenarios, one side is *not* justified in killing virtually any number of combatants to save one of its soldiers. I shall return to the latter scenario of killing many combatants to end the war below in the section on perspective in proportionality.

Returning to surveillance, and maintaining the analogy with the just war discourse, there are similarly three aspects of proportionality which should concern anyone engaged in surveillance. The first is the effects of surveillance as such (*jus ad speculandum*), the second is the effects of surveillance on those who are liable to be subject to surveillance (the proportionality principle of *jus in speculando*), and the third is the effects of surveillance on those who are not liable to be subject to surveillance (the proportionality qualification in the doctrine of double effect as a part of the principle of discrimination). The first of these was the subject under discussion in Chapter 10. The third, the doctrine of double effect, will be discussed in the following chapter on discrimination. In this chapter I focus on the proportionality of carrying out surveillance on the liable.

That it makes sense to talk of proportionality in terms of surveillance of the liable is, I suspect, less controversial than similar talk in war. Imagine that there are reasonable grounds to suspect a person of being an active shoplifter, and that shoplifting is an adequate offence to merit justified surveillance. Now imagine that the shoplifter is subjected to surveillance which would be more fitting for a suspected terrorist: 24/7 monitoring of personal movements, recording of all phone calls, bugs placed in his house, etc. Unless he were shoplifting something of value to national security this response would be entirely disproportionate. At the same time, it would be disproportionate also to subject a suspected terrorist to merely the level of surveillance which would be typical of that used against known shoplifters (say, generic CCTV with a heightened awareness on the part of the camera operator whenever the individual enters that operator's field of vision). If I am correct in this then it is possible for surveillance to be employed disproportionately against

legitimate targets, just as it is possible for acts of war to be employed disproportionately against legitimate targets.

This last consideration also highlights an ambiguity in the way in which "proportionality" is often used. In referring to surveillance as "disproportionate" the typical assumption, I suggest, is to imagine that it is excessive. However, this is not necessarily the case. It may be, as I have argued above, that it is inappropriate. This distinction can be illustrated by imagining a convicted rapist who has been punished with 40 hours of community service. This punishment is not excessive but it is certainly disproportionate. In this case the disproportionality arises from the inappropriateness of the punishment to the crime. It may be that an inappropriate matching of incident and response is excessive (e.g. receiving five years hard labour for stealing a loaf of bread), but it may also be that an inappropriate matching is not excessive (e.g. the rapist receiving community service). Hence proportionality refers to appropriateness, a subcategory of which is excessiveness. In this chapter I use the term proportionate to indicate appropriate and disproportionate to indicate something which is inappropriate, and not necessarily excessive.

I have already suggested a case which may be disproportionate when monitoring a liable person, namely wire-tapping the phone of a suspected petty shoplifter. In this case the subject of surveillance is liable (I shall assume for the purposes of the argument that petty shoplifting is a sufficient to justify surveillance) but the surveillance disproportionate. What is it that makes this surveillance disproportionate? On the other hand, why is incidental CCTV surveillance of a suspected violent terrorist also disproportionate? Bearing in mind the earlier definition, proportionality requires a balancing of harms and benefits such that the benefits outweigh the harms. It remains then, in seeking to answer these questions, to consider the relevant harms and benefits of particular acts of surveillance.

11.3 Harms and Benefits

11.3.1 Harms

In chapter 10 I argued that all harms arising from surveillance, as from war, should be considered in the balance of proportionality. What then are the harms of surveillance? To

an extent this question has already been addressed in Chapter 3, where I argued that the harms of surveillance could be dealt with in categories of individual and societal. The harms broke down into the following areas:

Societal

1. Chilling effects
2. Paternalism (harm to autonomy)
3. Social fatalism
4. Behavioural uniformity
5. Human error and abuse of power
6. Social sorting – stereotyping, stigmatization, discrimination
7. Imbalance of distribution of costs

Individual

1. Privacy violations
2. Vulnerability
3. Fear of control
4. Human error and abuse of power
5. Fear of being "found out" when hiding legitimate information

Each of these is discussed in greater depth in chapter 3. However, in this chapter I want to focus on one particular aspect: intrusiveness. As an act of surveillance becomes more intrusive so more, or more intimate, information is likely to be recovered on the surveilled subject. As more or more intimate information is recovered, so all of the harms listed above are likely to become either more likely to occur or they become greater harms when they do occur. Intrusiveness is therefore a key element in considering harms of surveillance.

To say that intrusiveness is a key element in considering harm is of limited use without clarifying what it is for an act of surveillance to be more or less intrusive. The question of intrusiveness can be illustrated through a consideration of the data returned by surveillance. Broadly speaking, surveillance can return two sorts of data: content and meta-data. In the case of a recording made of a meeting between two people, the content describes what was

said while the metadata describes the time, place and duration of the meeting. The value of meta-data and content respectively will depend on the context. If a target is a suspected terrorist talking on the phone about the location of a bomb about to be detonated then the content would be more valuable. If on the other hand the suspected terrorist is not talking about a wrongdoing then the number of the person to whom he is talking and the duration of the conversation may be of more use than the content. It will enable the surveillant to build up a picture of the terrorist's contacts and potentially find "middle men" who act as couriers between two terrorists. Such a middle man may convey information from one terrorist to the other allowing the two never to meet and so avoid being associated with one another. By then targeting the conversations of this middle man more intelligence may be gathered than by targeting either of the two terrorists themselves. Generally speaking, and depending on context, content can be useful for determining a person's intentions while metadata can give an understanding of that person's actions, their contacts and their habits, as well as building up profiles of people such that anomalous actions can be recognised (Kopstein 2013).

From the perspective of the individual or group affected, though, the collection of content will *usually* be more intrusive and thus more harmful than the collection of metadata. For many people, a close conversation between two individuals is the epitome of what is invoked by privacy. Hence types of surveillance which collect and record meta-data are intrusive, but those types which collect and record content are typically more intrusive still. As such, content-collecting types of surveillance are generally more harmful than those which collect just meta-data.

In conclusion to this section on harms, it can be said that a, if not the, key element to be considered is the intrusiveness of the particular form of surveillance. This underlies the severity of the harms experienced by surveillance. The more intrusive an act of surveillance, the more harmful it is likely to be.

11.3.2 Benefits

When looking at benefits in chapter 10, I argued that only two types of benefit should count in the balance. These were the sufficient just causes and contributing just causes. A third type of benefit, which I called peripheral benefits, should not count. Peripheral benefits are

those which benefit the surveillant but do not feature in the just causes. Hence the fact that Poole Borough Council would benefit from gaining employment for some of its staff in monitoring a family suspected of cheating the school allocation system should not count. This would be a peripheral benefit. That others may be dissuaded from cheating the school allocation system as a result of the surveillance would be, I held, a contributing just cause. The apprehension of the family suspected of cheating the system was the sufficient just cause and so should also count as a benefit when weighing proportionality.

In relating this line of thinking to the means of surveillance there is an obvious parallel in terms of peripheral benefits. I argued in chapter 10 that the contents of peripheral benefits and contributing just causes should be determined on a case-by-case basis, there being no unifying theory that would determine into which category a benefit fell. Intuitively, though, the benefit that a voyeur would gain from acting as a surveillant for a local council should not count in favour of the surveillance. The benefits should be more restrictive than that. However, there is a problem in that the just cause is an aspect of *jus ad speculandum* and yet the principle of proportionality currently under consideration falls under *jus in speculando*.

Michael Walzer holds that one should draw a clear separation between *jus ad bellum* and *jus in bello* considerations, rendering an ends-means distinction (Walzer 2006a; Walzer 2007). Hence those who declare war are responsible only for the declaration of war (the ends), while those who fight it are responsible only for how it is fought (the means). The result is that soldiers are not responsible for fighting in wars which have, for example, no just cause. They are merely responsible for how they fight in that war. While this may be the case in war (this is a highly controversial area and I will not attempt to address it here) it does not hold in surveillance.

Going back to the example of the violent terrorist, I will assume that a *jus ad speculandum* consideration has found surveillance to be acceptable in his case. All the relevant criteria have been met. The surveillant, in considering the ethics of the surveillance, must now turn to consider the *jus in speculando* aspects. The first of these is proportionality. However, in assessing the proportionality of the surveillance, the surveillant must surely bear in mind the wrongdoing that she is up against. Terrorism is a grave wrongdoing and could therefore justify very intrusive means of surveillance. In reaching this decision, though, the

surveillant is bringing the just cause of the surveillance to bear on her methods of surveillance.

This crossover between *jus ad speculandum* and *jus in speculando* has been implicit already in this chapter. The harms wrought by surveillance were considered in the context of harming a violent terrorist and a shoplifter. That is, the nature of the occasioning action (an aspect of just cause and hence *jus ad speculandum*) is *directly relevant* to the method of surveillance applied.

This being the case, I think that it is reasonable to take the benefits which can be weighed in the *jus in speculando* considerations of proportionality to fit the same categories as those in *jus ad speculandum*. Hence the relevant benefits are the sufficient just causes and contributing just causes. Peripheral benefits should not be counted in favour of the methods of surveillance just as they are not counted in favour of the ends of surveillance.

11.4 The Proportionality of Datong

In the introduction I raised a case of the Metropolitan police using a surveillance system known as Datong. According to the article from which I drew the case, this can pretend to be a mobile phone network with the subsequent abilities of turning off phones remotely, intercepting phone conversations and text messages, and gathering data about users in a targeted area. The article raised the question as to whether the system was proportionate.

The Datong system is, according to the article at least, potentially very intrusive. Phone calls and text messages are to many the epitome of private conversations. To intercept these is a violation of privacy which would need considerable justification in order to be acceptable.

To assess benefits one would normally apply the surveillance to the circumstances in which its use was proposed. Unfortunately neither Datong not the Metropolitan police would comment on actual situations in which the system has been used. Given this I will suggest three hypothetical scenarios: terrorists about to carry out an atrocity similar to the 7 July attacks in London; rioters such as took to the streets in August 2011; and shoplifters.

Taking the terrorists first, the intrusiveness of the surveillance is a considerable harm, but I shall presume that *in this case* the more intrusive the surveillance the more effective it will be. The benefits of the surveillance, if successful, would include apprehending the terrorists, avoiding the attack and thus saving dozens of people's lives, and deterring future terrorists from similar actions. This therefore strikes me at least as being proportionate.

Moving to the rioters, once again the surveillance is intrusive. The benefits of the surveillance include apprehending the wrongdoers, avoiding damage to property and endangerment of life, and deterring other rioters in the knowledge that their communications will be intercepted. The proportionality of this case is less clear-cut than that of the terrorist and would turn on the extent to which life and property were endangered by the rioters. The surveillance would be more likely to be proportionate as the risk of harm increases.

Finally there is the case of the shoplifter. Here the harms are intrusive as before. The relevant benefits include apprehending a petty criminal, preventing further shoplifting and deterring others from shoplifting. This strikes me as being clearly disproportionate.

11.5 Conclusion

In conclusion I have argued that proportionality affects both *jus ad speculandum* and *jus in speculando* considerations. That is, it is a proper consideration both in the decision whether to use surveillance (the ends) and in determining which type of surveillance to use (the means). In both cases, proportionality involves measuring and balancing the benefits and harms to arise from the surveillance. In this chapter I have argued that the *jus in speculando* harms consist in those harms visited on both the person placed under surveillance. The key consideration of harm is to be found in the concept of intrusiveness: the more intrusive an act, the more harmful it is likely to be.

In terms of benefits of particular acts of surveillance I argued against a strong separation between *jus ad speculandum* and *jus in speculando* considerations. The lack of a strong separation allows for the use of the same structure of benefits (i.e. sufficient just causes and contributing just causes) to be used for the principle of proportionality in *jus in speculando* as for the principle of proportionality in *jus ad speculandum*. Hence the benefits which can

be counted in weighing proportionality are the sufficient just causes and the contributing just causes, while peripheral benefits cannot be counted.

Finally I applied the considerations of proportionality raised above to the example of the Datong surveillance system. Without an example of how Datong has been used I suggested its use in three scenarios: against terrorists, against rioters and against a shoplifter. While its use against the terrorists was seen to be proportionate, its use against rioters was less clear. Proportionality in this case depended on the risk of harm presented by the rioters. Finally its use against the shoplifter was seen to be disproportionate.

This ends the two chapters looking at proportionality in surveillance. I turn now to second chapter in the section on *jus in speculando* and the final chapter of the thesis before the conclusion. This is the consideration of discrimination and the doctrine of double effect.

12. Discrimination

While it may feel as if surveillance is an omnipresent if diverse phenomenon, from the CCTV on the street corner to a neighbour with a compulsive habit of curtain twitching, establishing an ethical approach to surveillance is hampered by this very diversity. Even if we restrict ourselves to approaches that are panoptic (in which the few watch the many), as opposed to synoptic (in which the many watch the few), there are many approaches which may be typified as surveillance: peeping Toms; the use of wire taps, bugs, or telephoto lenses; being followed by car or on foot; CCTV; Automated Number Plate Recognition (ANPR); data collected through mobile phone networks or credit card usage; and so on.

One helpful way in which we can distinguish and categorise these diverse forms is through looking at who is being subject to surveillance in each case. In some instances there is a single person under surveillance, although the surveillant may in the process witness others with whom the subject interacts. Whether the surveillant chooses to put these others under surveillance is a further question. Such cases would typically include peeping Toms, wire taps and bugs. Other cases such as CCTV are more likely to monitor many people simultaneously, depending on where the surveillance is located. Some of these people may be of interest to the surveillant while others may not.

From this diversity arise questions as to whom should be monitored (the target), where and when should they be monitored (the location), and how to deal with the inadvertent monitoring of those who are not legitimate targets or surveillance (collateral damage). Consideration of each of these questions forms the parts of this chapter.

The first of these questions asks *who* should be subject to surveillance. Here there is a clear comparison which can be drawn with a war scenario in that both situations employ the semantics of targeting. In war one targets a person or group of people. In surveillance one also targets a person or group of people. It is establishing the identity of these people which is at issue. In both cases the dynamic is of *agent – target – subject*, with the notion of intentionally placing another in one's "sights" lying at the heart of each.

The question of who to target raises the principle of discrimination between legitimate and illegitimate targets. In war the combatant *should* discriminate between combatants

(legitimate targets) and non-combatants (illegitimate targets) on the basis of their wearing uniform and/or possession of a weapon (109th Congress 2006 sec. 948a; Pfanner 2004; Corcione 1991 p. 4; Nagel 1972 p. 140; US Supreme Court 1942). There is a parallel here in surveillance in that the surveillant *should* discriminate between legitimate and illegitimate targets. Legitimate targets are, I will argue, justified targets for surveillance while illegitimate targets are not justified.

I have already discussed the target in chapter 4 through looking at liability. I shall briefly expand upon the conclusions of chapter 4 here to demonstrate how liability relates to the legitimacy of a target.

The second question is a consideration of location (and, by extension, time). There are certain circumstances in which a particular location comes under surveillance rather than a particular person. In war such locations may include enemy headquarters or military barracks. Hence the location is chosen as it contains legitimate targets. Locations which contain no legitimate targets (nor are likely to) are not suitable for targeting. Harder to determine (and the subject of questions concerning collateral damage) are those places in which there are both legitimate and illegitimate targets present. In the context of surveillance this level of discrimination may be more challenging as legitimate targets are less likely to segregate themselves from illegitimate targets in the same way. Given this, is it legitimate to put a place under surveillance rather than a person? I argue that it is. In this argument I expand upon one minor area of chapter 4 regarding locations, rather than people, that are placed under surveillance. I argue that surveillance of a location is justified if there is reasonable evidence that there will be a person who may be treated as liable in that location during the period of the surveillance.

The third question concerns collateral damage. This occurs when illegitimate targets are directly affected by the targeting of legitimate targets. In both war and surveillance there are clearly cases with greater and lesser chances of collateral damage, depending on means and context. In war, a sniper may operate a rifle with a narrow scope (means) in an rural area (context), enabling him to target precisely one subject at a time. The chance of collateral damage from a single shot fired from a rifle is slim. By contrast a bomber (means) operating in an urban environment (context) lacks the same level of precision and is therefore more likely than the sniper to kill illegitimate targets.

The issue of collateral damage also carries into surveillance practice. Consider here surveillance which takes place in an individual's home (e.g. hidden cameras placed in the home of a suspected terrorist). This will lead to less collateral damage (the surveillance of illegitimate targets) than hidden cameras in a department store (Roberts 2012). The former location means that the surveillance is more likely to gather information on legitimate targets. The latter location means that the surveillance is more likely to gather information on illegitimate and maybe also legitimate targets. As such the *location* of a surveillance operation can have an effect on collateral damage.

At the same time the *means* of surveillance can also have an effect on collateral damage. Just as the sniper's rifle is more precise than the nuclear missile, so directional microphones recording two people's hushed conversation in a town square are more precise than non-zooming CCTV coverage of those two people in the same location. The directional microphone can be used to record solely the conversation of the two people, whereas the CCTV will record everyone in the specified location.

In discussing collateral damage I will draw on the doctrine of double effect (DDE) to establish when collateral damage is acceptable in surveillance. Here I shall draw on the argument presented in chapter 5 concerning intention. Recognizing that this approach is controversial, though, and without wanting to embark on a lengthy justification of the doctrine, I will suggest an alternative, albeit less satisfactory, approach for dealing with collateral damage.

Each of these areas of similarity between discrimination in surveillance and war (the target, the location, and collateral damage) forms the basis of the three parts to this chapter. The focus remains on surveillance, but owing to these similarities I continue to borrow from writings in the just war tradition to inform and clarify what discrimination is and how it should be employed.

12.1 The Target

In chapter 4, I established when there would be a justified cause to employ surveillance. This justified cause, I argued, was based either on the concept of liability or on the benefits significantly outweighing the costs. In this chapter I focus particularly on liability as

grounds for the just cause. It is not difficult to extend the argument to causes which are based on the benefits significantly outweighing the costs, but to state that in each case would be cumbersome.

I also drew a distinction between liability (a person has done or is intending to do some action which warrants surveillance as a means of detection or prevention) and being treated as liable (there is reasonable evidence of liability) in chapter 4. The default position for any person, I argued there, is that they are not liable for surveillance. They become liable only when they do something which warrants surveillance as a means of detection or prevention. However, that they have done something of this nature may not always be obvious to the surveillant. I therefore argued that the grounds for legitimacy of targeting were on evidence of liability. That is, when there is reasonable evidence of a person's being liable they may be treated as liable and may be targeted as such.

In extending this argument to the principle of discrimination there is a parallel to be drawn between liability and legitimacy. A person who is liable to be targeted in war is a legitimate target. Similarly, a person who is liable to be targeted in surveillance (or may be treated as such) is a legitimate target. Furthermore, if a person is not liable to be targeted in either war or surveillance (nor may they be treated as liable) then that person is an illegitimate target and so should not be targeted.

Considering the difference between legitimacy in both war and surveillance, there is a default position in both that a person is not a legitimate target. I argued in chapter 4 that a person must do something in order to become liable (legitimate) for targeting. In war that person must wear a uniform and/or carry a gun to become a legitimate target.[17] In surveillance that person must at the very least be implicated by reasonable evidence that they intend to commit or have committed an action which warrants surveillance. That is, there must be grounds for treating that person as liable in order for that person to be a legitimate subject for targeting by surveillance.

[17] I accept that this is an oversimplification. There is debate as to precisely who should be considered a legitimate target in war. See for example (Frowe 2011a), whereas I am drawing on the Geneva Protocols of the International Committee of the Red Cross (ICRC 1977). However, this debate does not affect my argument that there is a distinction between legitimate and illegitimate targets, merely the content of those categories.

By virtue of the default position, it is wrong to target any person if there are no grounds for treating him as liable for surveillance. As it is wrong to target a person who is not treatable in this way two areas of difficulty arise. The first of these is when it is a place that is put under surveillance rather than a person (e.g. a shopping mall). This is problematic as there may not be a legitimate person present during the surveillance but there could be illegitimate people present. The second is the problem of collateral damage, arising from the surveillance of people other than the legitimate target. In both cases the problem is that illegitimate people may be directly affected or targeted by surveillance.

12.2 The Location

As noted above, and referred to in chapter 4, there is a problem with some approaches to surveillance in that they appear to target locations rather than people. Take for instance CCTV for security in a shopping mall, in which the CCTV operator monitors the mall whether there is anyone there or not. Clearly a location cannot itself be liable for surveillance. The surveillance is carried out in anticipation of there being a person who is liable for surveillance. Although I shall continue to refer to the surveillance of places for convenience, I take it that the place itself is not the subject of surveillance but rather the people likely to use that place. Furthermore, as noted in the introduction, by location I am here referring to time and place. Nonetheless, it may be the case that the majority of the people likely to be seen by the CCTV operator watching over the shopping mall are not liable. Can such surveillance be justified?

While the above section focused on the person who can be legitimately targeted, here I look at the places and times when general surveillance is justified. While in these situations there is not necessarily an identified person or people present, the circumstances are such that a justified cause for surveillance may, or is *likely* to, occur. Hence shopping malls are places where shoplifters operate and so shoplifting may, or is likely to, occur. Similarly businesses where money or valuable items may be located may, or are likely to, be targeted by thieves and major public events such as the London Olympics or the Boston Marathon may, or are likely to, be targeted by terrorists. In each of these situations, an action warranting surveillance by some unspecified person is a reasonable likelihood. Is this context sufficient to justify surveillance, though?

A complicating factor here is that there are some actions which warrant surveillance, such as terrorism, which seek to cause devastation at times and places least expected. To a terrorist, all times and all places are possible targets. So to use surveillance in apprehending a terrorist, all times and all places become desirable as legitimate locations. This may lead to a push by some for Total Information Awareness (TIA) – as much surveillance coverage of a state and its people as possible, brought together in a single searchable database (Markoff 2002). Yet while this attracts some it terrifies others, who worry about the potential abuses of the state being given so much power (see chapter 3).

The question to be addressed in this section is whether surveillance is justified if it is only the location which is legitimate and not (necessarily) the people in that location? I shall argue that it is, *if* the location is justified by reasonable evidence that someone (for whom there are reasonable grounds for treating as liable) will use that location.

There is a clearly case to be made in favour of monitoring (some) places. There may be instances in which information reveals that an action warranting surveillance will occur in a particular location and at a particular time, but not the people involved. In these cases surveillance would be justified.

The same can be said of instances in which intelligence suggests that the same action is *likely* to occur. That is, if there is reasonable evidence that a person will carry out an action which warrants surveillance (as discussed in chapter 4) in a particular location, then that location may be justifiably subject to surveillance in order to apprehend or deter that person.

By contrast, surveillance of a location in which it was somehow known that no such action is likely to occur would be unjustified. While it is not immediately obvious as to what this would mean in real life, we could imagine a town in which there were no liable people as an hypothetical instance. Hence, as with targeting people, the justification for surveillance of places rests on the quality of evidence that the location is one which is likely to be used by a liable person (or one treatable as such), the surveillance of which could deter or apprehend that person.

Precisely how evidence is to be evaluated will be specific to each situation, and so not appropriate for discussion here. However, past behaviour in similar contexts could count as reasonable grounds for justification, along with current intelligence indicating a likelihood of future threats. Therefore if a shopping centre has repeatedly been subject to vandalism in the past, and that scale of vandalism is felt to warrant surveillance, then the shopping centre would be a justified location for surveillance even in the absence of specific intelligence indicating that more vandalism was likely.

There is a danger here of abuse. I am arguing that if a place has in the past been the location of an action warranting surveillance, or if intelligence suggests that it is likely to be such a location in the future then surveillance is justified. I have also argued that terrorism seeks to affect locations which are least expected (for example, the Guilford and Birmingham pub bombings in 1974, or the World Trade Centre in 2001). Indeed, it is almost a defining tactic of terrorists that they seek to instil fear (terror) into people's everyday lives in order to achieve their political goals. To achieve this they focus their attacks on "soft targets" which are poorly protected and will cause fear among the public. Such attacks are also often required by the limited resources of the terrorist organisations themselves, which may be such that they are unable to contemplate open confrontation with the state. Given that terrorists could target any place at anytime, could terrorism justify the ubiquitous surveillance of locations?

The key factor here is the term "likely". Certainly there are times (when a state is the target of an active terrorist group) when an attack on almost anywhere is possible. However, for an attack to be likely requires more than just a mere possibility. This does require intelligence in order to determine either when or where an attack is likely. Although perhaps imperfectly applied, this is to some extent captured by the terror alert levels employed by the US and UK governments after the 9/11 attacks.

Furthermore it is worth remembering that a justified cause is not the only consideration. For surveillance to be justified there are also be conditions of intention, chance of success, necessity, and proportionality which must be met. In the above case of TIA justified by possible acts of terrorism, it may be that while the acts remain possible and not likely the conditions of necessity and proportionality will not be met.

A second problem attendant on surveillance by context is that this may simply lead to a relocation of the justifying cause (Gill & Spriggs 2005 p. 2). Imagine that drugs were being dealt in a particular park at night. In response the local council installs infra-red CCTV cameras which will only operate at night. In all likelihood those dealing the drugs will relocate to a different park which does not have such surveillance. If the council places cameras at the new park, but takes them down at the old, then the dealers will relocate to their former location. If the council places cameras at every park the dealers will find somewhere other than parks for their business. As the council follows the dealers, installing new cameras as they go, so the local area becomes subject to a localised version of TIA.

It should be remembered here that surveillance is not a panacea for society's ills. Surveillance alone will not bring an end to the dealing in or taking of drugs. Hence surveillance needs to be used in co-ordination with other measures to respond to crimes or other social problems. While the installation of cameras may remove the problem from one area, which may be sufficient for some, the saturation of an area by CCTV cameras alone is unlikely to resolve the problem (Gill & Spriggs 2005 p. 118). The underlying issues leading to drug abuse or social problems will remain. As such surveillance is a sticking plaster to address the visible wound rather than medicine to cure the disease. To prevent the phenomenon of relocating crime, then, more than surveillance is necessary.

In conclusion, location can be used to justify surveillance if there is reasonable evidence to suggest that the location is likely to be one in which an act warranting surveillance will occur or which will be used by a person who may be treated as liable for surveillance. There is an acknowledged danger that justifying surveillance by context is open to abuse and could lead to attempts to saturate an area in surveillance to gain total information awareness. This could happen quickly, as in the case of terrorism, or through creep by following crime as it relocates in response to surveillance.

12.3 Collateral Damage

I have argued that both a person and a location can form legitimate targets. What, though, of those who are not legitimate targets but who are caught in the camera's eye (or bug's ear) nonetheless? The friend who speaks to the Mafia don's wife on the phone, not

knowing that the phone is bugged; or the mother with no ill intent walking in front of a CCTV camera in a public area. While the Mafia don and the public area are, or may be, legitimate targets, such surveillance is likely to result in the surveillance of those who are illegitimate targets. Not only are they illegitimate, they are generally unwanted by the surveillant. That is, the surveillance of such people would not form a legitimate intention for surveillance, as discussed in chapter 5. In war the unintentional killing of non-combatants (illegitimate targets) has become known as "collateral damage". The term serves adequately to be carried into the context of surveillance to similarly describe those who are not legitimate targets but are monitored even so.

I have argued that there are justifiable reasons for targeting people or places, if those people or places are legitimate targets. However, in both of these cases, as noted above, there is a possibility if not a likelihood of monitoring other, illegitimate targets. How should such "collateral damage" be dealt with? Is it enough to render the surveillance unjustified?

Keeping to the analogy with the principle of discrimination, when such collateral damage occurs in war it is frequently justified by appeal to the doctrine of double effect. It will be remembered from chapter 5 that the principle of discrimination states that non-combatants should not be targeted in war. However there are situations in which non-combatants will almost certainly be killed. In such cases the just war tradition has sought to offer guidance as to whether and how such situations could be accommodated. To this end, appeal has often been made to the doctrine of double effect (DDE), which sets out conditions to be met in order for the harm brought on non-combatants to be ethically legitimate. This raises the question as to whether the DDE could play a similar role in determining the employment of surveillance in situations where there is a likelihood of monitoring illegitimate targets. That is to say, although a surveillant may not target someone who may not be treated as liable, are there considerations which would allow for that person to be monitored, albeit not targeted? To answer this I shall consider two questions: does the DDE work; and if so, can appeal be made to the DDE in surveillance as it is in war?

The *locus classicus* of the DDE is found in Aquinas, who introduced a version of it when querying whether a person could justifiably kill in self-defence (Cavanaugh 2006 p. 2; Aquinas 2000 pp. 1465–66). It was developed by later commentators but took on a new urgency in the twentieth century, when developments in medical and martial technology

reintroduced concerns addressed by the doctrine. More recently the DDE has been critiqued by Thomas Scanlon, who argues that the intentions of agents (a central consideration of the DDE) are relevant to considerations of the agent's decision making process but not the moral permissibility of the action itself. As such, he claims, the DDE has little to say on the permissibility of an action.

I have dealt with Scanlon's claims in depth in chapter 5, so will not revisit them here. On the basis of my conclusions in that chapter, I will assume in this section that Scanlon's argument fails to convince. Here I shall offer a brief overview of the DDE before reviewing its value and whether it might provide justification for collateral damage in surveillance. In the event of my critique of Scanlon not being persuasive, though, I shall also consider an alternative approach which, I argue, is effective although not as satisfactory as DDE in resolving this issue.

12.3.1 Principles

As noted, the DDE can be traced back to Aquinas's discussion of killing in self-defence (Aquinas 2000 pp. 1465–66). Aquinas asks whether, given that killing a person would normally be wrong, this would continue to be the case if that killing were done in self-defence. As T.A. Cavanaugh points out, this is a comparatively brief discussion but still it is possible to see certain traits emerge which are central to later thinking on the DDE: firstly that there is a wide-ranging moral norm which, in a particular context, presents an intuitively difficult case; secondly that in considering the permissibility of the act we must consider the agent's intention; and thirdly that it is possible to generalize from Aquinas's account to form principles which establish when one might engage in an act which would itself be permissible (i.e. defending oneself) but which has foreseeable negative or evil consequences (i.e. killing another person) (Cavanaugh 2006 p. 12). That is to say, the DDE from its inception addresses the question of whether an act is permissible when there are foreseeable negative consequences. Such consequences in the case I am considering here would include collateral damage through incidental surveillance of illegitimate targets.

Through discussion of further challenging cases, commentators on Aquinas abstracted and developed these principles until 1850 when Jean-Pierre Gury presented the DDE in what is generally taken as its contemporary form such that:

1. the act in itself is good or indifferent;
2. the agent intends the good effect and not the evil effect;
3. the good effect is not produced by the evil effect; and
4. there is a proportionately grave reason for causing the evil effect (Cavanaugh 2006 p. 25).

Through a consideration of Gury's formulation, Cavanaugh finds that while he can support the first and last principles, the second and third are, when taken together, effectively tautologous. If, as suggest by principle 3, the evil effect (EE) were necessary for the good effect (GE) then in order to intend GE the agent would have to intend EE as well. But the agent's intending EE has already been ruled out by principle 2 (Cavanaugh 2006 pp. 30–1). Therefore, Cavanaugh concludes, and I agree, we can dispense with the third principle altogether. This leaves a revised formula as follows:

1. the act in itself is good or indifferent;
2. the agent intends the good effect and not the evil effect;
3. there is a proportionately grave reason for causing the evil effect (Cavanaugh 2006 p. 36).

As noted, there have traditionally been a number of scenarios posed in which the DDE is employed to evaluate the outcome. In the following, I will discuss one common example, that being the difference between terror bombing and strategic bombing. The scenario at its most basic posits that a pilot is flying over enemy territory with the aim of dropping a bomb on the enemy's military headquarters. However, the enemy HQ is situated next to a school so that by dropping the bomb on the HQ the children in the school will die, killed by the blast of the bomb. Clearly there is a potential advantage to the war effort if the children die as this will likely lower enemy morale and so hasten the end of the war. Despite this, most people recoil at the idea of a bomber deliberately killing children (this would be to target illegitimate targets and therefore wrong) and so the question is asked whether the pilot intends to destroy the HQ and merely foresees the deaths of the children. If so then the pilot is considered to be a strategic bomber (SB). SB is taken by the DDE to be morally permissible. If on the other hand the pilot intends to destroy both the HQ and the children then he would be considered to be a terror bomber (TB). TB is taken by the DDE to be morally impermissible.

The only difference between SB and TB is the intention of the pilot. According to the DDE, though, this is hugely significant. The fact that SB does not *intend* the deaths of the

children justifies his actions. By contrast, the fact that TB does intend the deaths of the children renders his actions unjustified.

As noted, there is a common sense of recoil at the scenario presented by TB. A further advantage of the DDE is that it highlights what it is that is objectionable about TB. Although the effects are the same in both, the central difference is in the intention of the pilot in either destroying a legitimate military location or in deliberately killing children. While tragedies do occur in war, it is hoped that all those involved in the fighting also see them as tragedies and act to avoid them where possible.

12.3.2 DDE and Surveillance

Although less severe than war, in that no-one usually dies as a direct result of surveillance, there is a straightforward analogy between SB/TB and a similar issue in surveillance. In both cases, it will be remembered, we are operating in the realm of *jus in bello*, that is at the level of the operator rather than the overall decision to go to war or employ surveillance. Hence the concern is with how the operator functions when using the equipment of surveillance, or the choices the operator makes in deciding which form of surveillance to employ. However, this equipment is often indiscriminate in its operation: when a bomb is dropped it is not known exactly who will be underneath it; when CCTV is operated in a shopping mall it is similarly unknown as to who will walk in front of it. The principle of discrimination, though, argues that the operator should discriminate between legitimate and illegitimate targets. As such, it might seem as if any means which is indiscriminate must be avoided or even prohibited.

Keeping with the analogy between SB/TB and CCTV, imagine that the surveillant's target is a criminal who is known to operate in a public space (say, a shoplifter in a supermarket). The operation will result in the collecting of information about that criminal, *vice* his immediate death in the case of SB/TB. It will also, because of the indiscriminate nature of the equipment, result in the collection of information about a number of illegitimate targets. I shall also hold conditions 1 and 3 to be constant so that, as in the SB/TB distinction, it is only the intention of the agent that is different in the two cases.

To draw the analogy in surveillance with SB, imagine a CCTV operator who does not intend to carry out surveillance on illegitimate targets. I shall call him Good Operator (GO). GO is similar to the SB as the consequence resulting from a justified intention coupled with an indiscriminate approach is the foreseeable harm of a number of illegitimate targets. In both cases, the effects which are intended for a legitimate target are, as a consequence of the operation, foreseeably meted out on a number of illegitimate targets.

By contrast, the analogy with TB would be for the CCTV operator to intentionally collect information on those people ordinarily considered to be illegitimate targets. I shall call him Bad Operator (BO). BO's intentions could be realised either by employing the tool when it is known that there are no shoplifters present, or by employing the tool so that legitimate and illegitimate targets are surveilled simultaneously. The reasons for such a decision are as numerous and varied as for the pilot in TB (who might wish to end the war through destroying enemy morale, or just might have a sick streak such that he enjoys murdering children), but might include voyeurism on the part of BO.

The DDE would therefore justify the actions of GO but condemn those of BO. It can also clarify why it is that there may be a common sense that GO's actions are legitimate while BO's are not, even though the consequences are identical. A further value of the DDE is that it also establishes the importance of proportionality in such actions, but does so while recognizing strict limits which should not be transgressed.

To return to the three principles of the DDE, these are:

1. the act in itself is good or indifferent;
2. the agent intends the good effect and not the evil effect;
3. there is a proportionately grave reason for causing the evil effect.

Keeping with the example of the shoplifter in a supermarket, the act in this case is to detect shoplifting. This is, I will assume, a good act. Shoplifting is wrong and shoplifters should be apprehended and dealt with accordingly. The act with negative consequences is the surveillance of law-abiding shoppers in the supermarket. I will assume here that the operator intends the good effect (apprehending the shoplifter) and not the evil effect (surveillance of law-abiding customers). Finally, the doctrine demands that there be a

proportionate reason for causing the evil effect. That is, the harm caused by the shoplifter must outweigh the harm caused to the law-abiding customers.

The DDE hence has several functions within the principle of discrimination. Firstly it introduces intention as a *jus in speculando* consideration. Intention is a part of *jus ad speculandum*, as noted in chapter 5, but only appears as a consideration in determining the *means* of war in the DDE. Against Scanlon's objections to the contrary, I have argued that intention is a morally relevant consideration in relation to the principle of discrimination, that is, within the *in bello* considerations. Were the DDE to be abandoned then a principle of intention should be introduced elsewhere among the *jus in speculando* principles.

Secondly, the DDE introduced an important third element of proportionality into the overall analysis. Proportionality is a consideration in whether to employ surveillance (chapter 10), how to employ surveillance against legitimate targets (Chapter 11) and also, it can now be seen, in how to employ surveillance when the monitoring of illegitimate targets is unavoidable.

The DDE therefore answers the question of when, if ever, illegitimate targets can be subject to surveillance. The principle of discrimination asserts that they should never be targeted, but it is accepted that monitoring them is to some extent inevitable given the forms of surveillance employed. The DDE therefore serves as a restrictive argument which supports the principle of discrimination and supplements it with the further qualification of proportionality.

12.3.3 Non-DDE Alternatives

I have noted above that the DDE is not universally accepted. Much of chapter 5 is given over to a critique offered by Scanlon regarding the moral relevancy of intention as it appears in the DDE. For others there may be a suspicion that the DDE is somehow too easy: anyone could *say* after the event that they did not intend for the evil effect. Thirdly, taking a more consequentialist stance, the fact remains that innocents have been killed and this is wrong.

I have already said that I do not intend to mount a philosophical defence of the DDE in this chapter. Instead I will present what I see as being the two likely alternatives if the DDE is

rejected. The first of these is to focus on the proportionality of the action alone, which is where I see the conclusion of Scanlon's argument as leading, while the second will focus on the consequences of the action alone.

Take first the alternative of focusing on proportionality alone. In this case the moral relevance of intention is rejected. The prohibition of the principle of discrimination cannot therefore relate to targeting illegitimate targets, as this is an irreducibly intentional act (see chapter 5). Instead the principle of discrimination is most likely to relate to the harming of illegitimate targets. One option here is to see the harming of illegitimate targets as absolutely forbidden by the principle. This would mean that indiscriminate means of warfare such as bombs and missiles would be heavily restricted in their use. The same would be true of indiscriminate means of surveillance, such as CCTV. If there were a foreseeable chance that an illegitimate target would be harmed then such means should not be used. This is certainly a legitimate approach to take, but it is not a compelling conclusion. As I have argued above, there are a sufficient number of cases in which the use of CCTV seems justified, even though illegitimate targets will be subject to surveillance.

The second option presented by this approach is to say that the prohibition of harming illegitimate targets is not prohibited but should be minimized. This is to reduce the principle of discrimination to a principle of proportionality related to illegitimate targets. The result of this approach is to allow for the deliberate targeting of illegitimate targets provided that the benefits outweigh the costs. Applying this argument to war would result in condoning deliberate bombings of civilian populations if it could be deemed proportional to the concluding of the war. Where the British engaged in this activity during WWII it has subsequently been questioned and criticised (Hills 2013; Walzer 2006a pp. 255–68; Harding 2003a). The problem here is that mere proportionality is insufficient to provide the levels of protection in war that many seek. By analogy I suggest that it would be equally insufficient in the case of surveillance.

The second alternative would be to focus on consequences alone. In this there is no great difference from the "pure proportionality" approach suggested above. This, I hold, offers insufficient respect or protection for those we normally seek to protect from harm in times of war (i.e. children and the elderly). The results would be similar in surveillance and could be used to justify TIA or similar proposals for ubiquitous surveillance in the name of

security. In each of these cases, as in war, those for whom there were no grounds to treat as liable for surveillance would be treated as if there were such grounds. The attendant harms of surveillance would therefore be visited on a population more widely than would be the case with the DDE in operation.

Hence there are alternatives to using the DDE to justify collateral damage. However, these are inferior in quality to employing the DDE. The benefits of the DDE are that it limits the harms of surveillance more effectively than a consequentialist approach or one which proposes removing the prohibition on targeting illegitimate targets. At the same time it allows for surveillance which would unavoidably monitor some of those illegitimate targets at certain times in a way which merely upholding the principle of discrimination would not.

12.4 Conclusion

In this chapter I have sought to understand and explain the manner in which surveillance should be discriminating. To do this I have drawn on the principle of discrimination in the just war tradition. I argued at the outset that there are similarities between surveillance and war insofar as both involve targeting. From this a number of further similarities emerge regarding the target, the location and collateral damage. I then treated each of these in turn in the three parts of the chapter.

In looking at targets I argued that there are legitimate and illegitimate targets for surveillance. Drawing on the arguments in chapter 4, a legitimate target is a liable person, or one who may reasonably be treated as such. Owing to the harms of surveillance the default position of a person is that they are not liable for surveillance.

I then argued that surveillance can justifiably be targeted at locations. This arises when there is evidence that a particular location will be subject to activity which would justify surveillance. I considered the possibility of abuse through an attempt to apply surveillance to all locations and argued that surveillance was not a panacea, and so to treat it as a means to resolve social problems was likely to fail.

Finally I considered the issue of collateral damage, drawing on the doctrine of double effect. The DDE introduces two necessary considerations into *jus in speculando*: the intention of the operator of the equipment (and/or the person deciding which equipment to

use) and proportionality of the harm caused by the equipment on illegitimate targets. In this it was noted that proportionality therefore permeates just surveillance: at the *ad speculandum* level concerning whether to employ surveillance, the *in speculando* level concerning which method of surveillance to employ against legitimate targets, and the level of collateral damage, concerning the surveillance of illegitimate targets.

Part IV - Conclusion

13. Conclusion

As I claimed in the introduction, in this thesis I have attempted to convince the reader of three things. Firstly, that there is an analogy between the ethics of war and the ethics of surveillance insofar as the principles used in the just war tradition provide a comprehensive framework for analysing surveillance. Secondly, that the tradition can provide analysis helpful to understanding the principles and how they should be applied to surveillance. Thirdly, by drawing on the just war tradition I have offered a normative position to be taken on each of these principles. Each of these I develop below:

13.1 Principles

Where there has been academic discussion on the ethics of surveillance this has been limited and tentative. David Lyon, Graham Sewell and James Barker, Anita Allen and John Kleinig have all contributed to the debate in recent years (Kleinig 2009; Allen 2008; Lyon 2001; Sewell & Barker 2001), yet none has offered a comprehensive approach. The closest anyone has come to achieving this has been Gary Marx in listing 29 questions to ask of surveillance operations (Marx 1998). Yet even here, and by his own admission, Marx's list is a combination of empirical and normative questions, and lacks any theoretical coherence or underpinning.

In appealing to the just war tradition as a framework for analysing surveillance from an ethical perspective I have tried to answer the problems faced by the authors above. This framework neither misses out ethically significant factors which are overlooked by the above authors, nor does it introduce ethically irrelevant factors when it is applied to surveillance. This can be clearly seen by revisiting the table from chapter 2 (Table 5, below).

Consideration	Lyon	Sewell & Barker	RIPA	Kleinig	Marx	Allen	Just War Tradition
Cause	✓	✓		✓	✓	✓	✓
Authority	✓	✓	✓		✓		✓
Intention					✓		✓
Necessity		✓	✓	✓	✓		✓
Chance of Success				✓	✓		✓
Declaration of Intent					✓		✓
Proportionality	✓		✓	✓	✓	✓	✓
Discrimination			✓				✓
No means *mala in se*				✓			✓
Treatment of prisoners							✓

Table 5: Summary of Principles Applied to Ethics of Surveillance

Like the just war tradition, the framework I have proposed provides clear principles for analysis rather than always offering the content of that analysis. Hence in just war the principle of discrimination, for example, demands that non-combatants not be targeted without always clarifying exactly who should count as a non-combatant. Similarly in just surveillance there are principles which require further elaboration, such as the weight given to privacy concerns in the principle of proportionality. As such it is a comprehensive *framework*, unlike that of Lyon, Sewell and Barker, Allen, or Kleinig. Furthermore it is a thoroughly normative system developed and tested over centuries and so has what Marx refers to as the "Rosetta Stone" quality of an ethical system for surveillance, in that it is not only coherent and complete but carries with it philosophical rigour. If the reader agrees at

the end of this thesis that the just war tradition does supply such an analytic framework then I will consider my arguments to have been successful.

It may be noted that I have not addressed the minor principles of no means *mala in se* and the treatment of prisoners. This has been for considerations of space in this thesis, coupled with a desire to focus on the uncontroversial principles, rather than a lack of material. Indeed, the idea that there may be some surveillance which is *mala in se* raises some interesting questions. Are there people or places which should be forbidden for the surveillant, or particular means such as determining thoughts from brain scans (Calo 2013).

The relevance of treatment of prisoners is less obvious. However, an analogy could be drawn either to the surveillance of literal prisoners (i.e. those found guilty of actions warranting imprisonment by society through judicial process) or to the treatment of the data collected by surveillance. Both are intriguing paths to follow but, as minor principles in the just war tradition, do not demand treatment here in the way that the other principles do.

13.2 Philosophical Tradition

In using this approach to the ethics of surveillance, my desire has been to advance the subject by using philosophical tradition when it comes to developing ethical norms for surveillance. As a "new" subject the potential for discussion is such that it could take years to arrive at similar conclusions if we fail to learn from pertinent areas of philosophy. By acknowledging the similarities between the ethics of war and the ethics of surveillance, I have drawn on thousands of years of discourse to advance the literature in the field of surveillance ethics further than had it started from scratch. This can be seen from the following overview of the classic and contemporary just war literature used to inform each chapter:

Just Cause	In this chapter several commentators in the just war tradition (Hugo Grotius, James Turner Johnson, Thomas Nagel, Raymond de Peñafort, Christine de Pizan, Emer de Vattel, Christian von Wolff and Michael Walzer) were drawn upon to inform the notion of liability in war, which was then used to shape an understanding of liability in surveillance. Jeff McMahan's discussion of just causes in

	war was helpful in drawing a distinction between desert and liability and Whitley Kaufman's analysis of pre-emptive wars was similarly useful in understanding the role of evidence in establishing liability.
Intention	Here Thomas Scanlon's work on the moral relevance of intention and Jeff McMahan's reply were important in considering a serious challenge to this notion and why it ultimately fails in both war and surveillance.
Authority	Thomas Aquinas's work helped establish the reason for the importance of the authority condition in the just war tradition as limiting war to more responsible parties, rather than allowing private wars. This view was reinforced in the contemporary period by C.A.J. Coady and James Turner Johnson.
Necessity	This chapter drew heavily from John Lango's work in understanding the nature of the last resort condition and what is meant by necessity. In particular, Lango's two conditions of plausible alternatives and awfulness were instrumental in determining when an act of surveillance could be considered necessary.
Declaration	Marcus Tullius Cicero, Hugo Grotius and Samuel von Pufendorf each lent an understanding to the value of making formal declarations in war for providing an element of accountability, a value which carries over in the ethics of surveillance.
Chance of Success	None
Proportionality	These chapters drew from Thomas Hurka in gaining insight into which benefits and which harms should be weighed in the balance when considering whether or not an act of war, or, by extension, an act of surveillance, is justified. Furthermore, challenges raised by Michael Walzer and Oliver O'Donovan as to whether proportionality is a relevant or useful criterion were also considered.

Discrimination	In this chapter Helen Frowe, Thomas Nagel and Toni Pfanner were helpful in distinguishing between legitimate and illegitimate targets, as were statutes, international law and military rules of engagement. Thomas Aquinas also provided an underpinning for the doctrine of double effect, which was seen to have relevance to both war and surveillance.

It is noteworthy that one chapter (chance of success) did not explicitly draw on just war literature to inform the argument. This, though, is a principle not given to much discussion in the just war tradition. There is hence relatively little literature available, and none was seen to be necessary in this case owing to the intuitive strength of the principle. Just as it seems eminently reasonable that combatants should not be sent to die in vain, so it seems equally reasonable that surveillance should not be taken without a chance of achieving its end. I do not believe that there is need for further or deeper justification than this.

13.3 Normative Conclusions

Finally I have made substantive normative claims regarding surveillance. An overview of the claims made in each chapter follows:

Just Cause	All acts of non-consenting surveillance carried out on autonomous adults must have a just cause. This cause must derive from the liability of the person or place subjected to surveillance. Alternatively it may come in cases in which the benefit significantly outweighs the harms caused. Paternalist considerations, though, do not provide grounds for a just cause.
Intention	The intention of the surveillant in carrying out the surveillance is a morally relevant consideration and should be the same as the given just cause.
Authority	The surveillant should have authority to carry out surveillance. However, this condition is *pro tanto* rather than necessary. There are occasions in which a surveillant who is not an authority is justified in carrying out surveillance.

Necessity	The surveillance must be an act of last resort. There must either be no alternative to the surveillance in order to meet the just cause or the available alternatives must be more harmful than the surveillance itself.
Declaration	The surveillance should be declared either to the surveilled subject or to a higher authority. It is *pro tanto* better the more people to whom the surveillance is declared in order that the surveillant be held to account for the surveillance. As with authority, though, this is not a necessary condition.
Chance of Success	The surveillance must have a chance of succeeding in achieving the just cause. Gratuitous surveillance is morally unacceptable.
Proportionality (*jus ad speculandum*)	The benefits derived from the just cause for surveillance and contributing benefits must clearly outweigh the harms of that surveillance. Peripheral benefits should not be weighed in the balance.
Proportionality (*jus in speculando*)	The benefits derived from the method of surveillance in meeting the just cause for surveillance and contributing benefits must clearly outweigh the harms of that surveillance. Again, peripheral benefits should not be weighed in the balance.
Discrimination	Surveillants must discriminate between legitimate and illegitimate targets. They must not target illegitimate targets, although the doctrine of double effect allows for the unintended monitoring of illegitimate targets under certain conditions.

References

109TH CONGRESS 2006. *Military Commissions Act*.

ALLEN, A.L. 2008. The Virtuous Spy: Privacy as an Ethical Limit. *The Monist*. **91**(1),pp.3–22.

ALLEYNE, B.R. 2008. Poole council spies on family over school claim. *Telegraph.co.uk* [online]. Available from: http://www.telegraph.co.uk/news/uknews/1584713/Poole-council-spies-on-family-over-school-claim.html [Accessed July 19, 2012].

AMNESTY INTERNATIONAL 2011. Impunity and attacks silence Russian journalists. Available from: http://www.amnesty.org/en/news-and-updates/impunity-and-attacks-silence-russian-journalists-2011-10-13 [Accessed July 29, 2013].

ANON 2012. NSA 60th Anniversary. Available from: http://www.nsa.gov/about/cryptologic_heritage/60th/index.shtml.

ANSCOMBE, E. 2006. The Justice of the Present War Examined *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Ox: Blackwell Publishing, pp. 630–32.

AQUINAS, S.T. 2000. *Summa Theologica* New edition. Resources for Christian Living,US.

AUGUSTINE 2006. City of God *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 80–81.

BACZYNSKA, G. 2009. Poland okays forcible castration for pedophiles. *Reuters* [online]. Available from: http://www.reuters.com/article/2009/09/25/us-castration-idUSTRE58O4LE20090925 [Accessed July 26, 2013].

BALL, K. et al. 2006. *A Report on the Surveillance Society*. London: Information Commissioner's Office.

BAMFORD, J. 1982. *The Puzzle Palace: A Report on NSA, America's Most Secret Agency* 5th THUS. Houghton Mifflin.

BARR, A. 2008. The Surveilled Realm. *Proudly Serving My Corporate Masters* [online]. Available from: http://www.proudlyserving.com/archives/2008/06/the_surveilled.html [Accessed July 13, 2013].

BARRETT, D. 2012. Phone and email records to be stored in new spy plan. *Telegraph.co.uk* [online]. Available from: http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html [Accessed August 19, 2012].

BATTY, D. 2009. Timeline: Baby P case. *The Guardian* [online]. Available from: http://www.guardian.co.uk/society/2009/may/22/baby-p-timeline [Accessed July 26, 2013].

BENN, S. 1971. Privacy, freedom, and respect for persons *In*: J. PENNOCK and R. CHAPMAN, eds. *Nomos XIII: Privacy*. New York: Atherton Press.

BEST, A. et al. 2008. *International History of the Twentieth Century and Beyond* 2nd ed. Abingdon, Oxon; New York: Routledge.

BIG BROTHER WATCH 2011. *Local Authority Data Loss* [online]. London: Big Brohter Watch. Available from: http://bigbrotherwatch.org.uk/la-data-loss.pdf [Accessed November 24, 2011].

BOETHIUS, A.M.S. 1969. *The Consolation of Philosophy* New edition. Penguin Books Ltd.

BOND, D. and M. MCDUGALL 2009. *Erasing David*. NHK BS1.

BOYD, danah 2010. Making Sense of Privacy and Publicity *In*: Austin, Texas. Available from: http://www.danah.org/papers/talks/2010/SXSW2010.html.

BRANDT, R.B. 1972. Utilitarianism and the Rules of War. *Philosophy and Public Affairs*. **1**(2),pp.145–165.

CALO, M.R. 2013. Brain Spyware. *Concurring Opinions* [online]. Available from: http://www.concurringopinions.com/archives/2013/04/brain-spyware.html [Accessed July 30, 2013].

CAVANAUGH, T.A. 2006. *Double-Effect Reasoning: Doing Good and Avoiding Evil*. Oxford: Clarendon Press.

CHANNEL 5 BROADCASTING LTD 2011. Big Brother. *Official Big Brother UK* [online]. Available from: http://www.facebook.com/bigbrotheruk [Accessed July 6, 2013].

CHISHOLM, N. and G. GILLETT 2005. The patient's journey: Living with locked-in syndrome. *BMJ*. **331**(7508),pp.94–97.

CICERO, M.T. 2006. On Duties *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 50–59.

CLULEY, G. 2013. Is it ever acceptable for a journalist to hack into somebody else's email? *Naked Security* [online]. Available from: http://nakedsecurity.sophos.com/2013/03/19/is-it-ever-acceptable-for-a-journalist-to-hack-into-somebody-elses-email/ [Accessed March 23, 2013].

COADY, C.A.J. 2007. *Morality and Political Violence* 1st ed. Cambridge University Press.

COATES, A.J. 1997. *The Ethics of War*. Manchester University Press.

COLUMBIA LAW REVIEW 1969. The Chilling Effect in Constitutional Law. *Columbia Law Review*. **69**(5),pp.808–842.

CORCIONE, G.D. 1991. Manuale di diritto umanitario, Introduzione e Volume I, Use e conventioni di Guerra, SMD-G-014, Stato Maggiore della Difesa, I Rparto, Ufficio Addestramento e Regolamenti, Rome, Vol 1, S4.

COUNCIL OF EUROPE 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14* [online]. Available from: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm [Accessed June 13, 2011].

DICK, P.K. 2000. *Minority Report* New Ed. Gollancz.

DODD, V. 2010. Stop and search plans are 'discriminatory', watchdog warns. *The Guardian* [online]. Available from: http://www.guardian.co.uk/uk/2010/nov/15/stop-and-search-equality-commission [Accessed March 31, 2011].

DOYLE, T. 2009. Privacy and Perfect Voyeurism. *Ethics and Information Technology*. **11**,pp.181–189.

DROGIN, B. 2008. *Curveball: Spies, Lies and the Man Behind Them: The Real Reason America Went to War in Iraq*. Ebury Press.

DUHIGG, C. 2012. How Companies Learn Your Secrets. *The New York Times* [online]. Available from: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [Accessed March 19, 2012].

FEINBERG, J. 1986. *Harm to Self*. Oxford University Press, USA.

FEINBERG, J. 1988. *Harmless Wrongdoing*. Oxford University Press.

FICKLING, D. 2006. Cannibal killer gets life sentence. *the Guardian* [online]. Available from: http://www.guardian.co.uk/uk/2006/may/09/ukcrime.world [Accessed February 16, 2013].

FISCHER, B.B. 2007. The Katyn Controversy: Stalin's Killing Field. *The Katyn Controversy: Stalin's Killing Field* [online]. Available from: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art6.html [Accessed August 19, 2012].

FRITH, M. 2004. How average Briton is caught on camera 300 times a day. *The Independent* [online]. Available from: http://www.independent.co.uk/news/uk/this-britain/how-average-briton-is-caught-on-camera-300-times-a-day-572781.html [Accessed March 9, 2013].

FROWE, H. 2011a. Self-Defence and the Principle of Non-Combatant Immunity. *Journal of Moral Philosophy*. **8**,pp.530–546.

FROWE, H. 2011b. *The Ethics of War and Peace: An Introduction*. Routledge.

FUNDER, A. 2004. *Stasiland: Stories from Behind the Berlin Wall* New edition. Granta Books.

GALLAGHER, R. and R. SYAL 2011. Met police using surveillance system to monitor mobile phones. *the Guardian* [online]. Available from: http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance [Accessed August 20, 2012].

GAVISON, R. 1984. Privacy and the limits of the law *In*: F. D. SCHOEMAN, ed. *Philosophical Dimensions of Privacy*. Cambridge: Cambridge University Press, pp. 346–402.

GIACOMO, D.F. (ed.). 2011. *The Eu Charter of Fundamental Rights*. Springer.

GILL, M. and A. SPRIGGS 2005. Assessing the Impact of CCTV. Available from: http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf [Accessed July 26, 2010].

GILLIAM, T. 1985. *Brazil*. Universal Pictures.

GLOVER, J. 1990. *Causing Death and Saving Lives: The Moral Problems of Abortion, Infanticide, Suicide, Euthanasia, Capital Punishment, War and Other Life-or-death Choices* New Ed. Penguin.

GRAHAM, G. 1996. *Ethics and International Relations*. Wiley-Blackwell.

GRAHAM, S. 1998. Towards the Fifth Utility? On the Extension and Normalisation of Public CCTV *In*: Clive NORRIS, J. MORAN and G. ARMSTRONG, eds. *CCTV, Surveillance and Social Control*. Aldershot: Ashgate Publishing Limited.

GROTIUS, H. 2006. On the Law of War and Peace *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 387–437.

GROVIER, T. 1982. What's Wrong with Slippery Slope Arguments? *Canadian Journal of Philosophy*. **12**(2),pp.303–316.

HADJIMATHEOU, K. 2013. The Relative Moral Risks of Untargeted and Targeted Surveillance. *Ethical Theory and Moral Practice*. **16**.

HARDING, L. 2003a. Germany's forgotten victims. *the Guardian* [online]. Available from: http://www.theguardian.com/world/2003/oct/22/worlddispatch.germany [Accessed July 30, 2013].

HARDING, L. 2003b. Victim of cannibal agreed to be eaten. *the Guardian* [online]. Available from: http://www.guardian.co.uk/world/2003/dec/04/germany.lukeharding [Accessed February 16, 2013].

HARWOOD, M. 2010. Terrorists Slip Past TSA's Scientifically Untested Behavioral Threat Detection Program. *Security Management* [online]. Available from: http://www.securitymanagement.com/news/terrorists-slip-past-tsas-scientifically-untested-behavioral-threat-detection-program-007158.

HASTINGS, R. 2012. New HD CCTV puts human rights at risk. *The Independent* [online]. Available from: http://www.independent.co.uk/news/uk/crime/new-hd-cctv-puts-human-rights-at-risk-8194844.html [Accessed August 13, 2013].

HILLS, S. 2013. 'I would have destroyed Dresden again': Bomber Harris was unrepentant over German city raids 30 years after the end of World War Two. *Mail Online* [online]. Available from: http://www.dailymail.co.uk/news/article-2276944/I-destroyed-Dresden-Bomber-Harris-unrepentant-German-city-raids-30-years-end-World-War-Two.html [Accessed July 30, 2013].

HOME OFFICE 2010. Covert Surveillance and Property Interference Revised Code of Practice. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf [Accessed June 14, 2013].

HOPE, C. 2010. Number of crimes caught on CCTV falls by 70 per cent, Metropolitan Police admits. *Telegraph.co.uk* [online]. Available from: http://www.telegraph.co.uk/news/uknews/crime/6867008/Number-of-crimes-caught-on-CCTV-falls-by-70-per-cent-Metropolitan-Police-admits.html [Accessed June 14, 2013].

HOPE, C. 2009. One crime solved for every 1,000 CCTV cameras, senior officer claims. *Telegraph.co.uk* [online]. Available from: http://www.telegraph.co.uk/news/uknews/crime/6081549/One-crime-solved-for-every-1000-CCTV-cameras-senior-officer-claims.html [Accessed June 14, 2013].

HUME, D. 2008. Of the Original Contract *In*: S. COPLEY and A. EDGAR, eds. *Selected Essays*. Oxford: Oxford Paperbacks.

HURKA, T. 2005. Proportionality in the Morality of War. *Philosophy and Public Affairs*. **33**(1),pp.34–66.

HUXLEY, A. 2007. *Brave New World*. Toronto: Vintage Canada.

ICRC 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). Article 44.3. Available from: http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=524284F49042D4C8C12563CD0051DBAF [Accessed May 10, 2013].

IGNATIEFF, M. 2004. Lesser Evils. *The New York Times* [online]. Available from: http://www.nytimes.com/2004/05/02/magazine/02TERROR.html [Accessed November 24, 2011].

JARVIS, J. 2011. *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*. Simon & Schuster.

JOHNSON, J.T. 2007. Just War Thinking in Recent American Religious Debate over Military Force *In*: C. REED and D. RYALL, eds. *The Price of Peace*. Cambridge: Cambridge University Press, pp. 76–97.

JOHNSON, J.T. 2000. Maintaining the Protection of Non-Combatants. *Journal of Peace Research*. **37**(4),pp.421–48.

JOHNSON, J.T. 1999. *Morality and Contemporary Warfare*. Yale University Press.

JOHNSON, W. 2012. CCTV used in more than 200 school toilets. *The Independent* [online]. Available from: http://www.independent.co.uk/news/uk/home-news/cctv-used-in-more-than-200-school-toilets-8129979.html [Accessed March 2, 2013].

JORDAN, D. 2011. The BBC and private investigators. Available from: http://www.bbc.co.uk/blogs/theeditors/2011/03/the_bbc_and_private_investigat.html [Accessed March 2, 2013].

KANE, C. 2011. Newspapers guilty of contempt in Joanna Yeates murder probe. *Reuters* [online]. Available from: http://uk.reuters.com/article/2011/07/29/uk-britain-jefferies-libel-idUKTRE76S20X20110729 [Accessed January 12, 2012].

KAUFMAN, W. 2005. What's Wrong with Preventive War? The Moral and Legal Basis for the Preventive Use of Force. *Ethics & International Affairs*. **19**(3),pp.23–38.

KETEYIAN, A. 2010. TSA's Program to Spot Terrorists a $200M Sham? *CBS Evening News* [online]. Available from: http://www.cbsnews.com/stories/2010/05/19/eveningnews/main6500349.shtml [Accessed May 17, 2011].

KLEINIG, J. 2009. The Ethical Perils of Knowledge Acquisition. *Criminal Justice Ethics*. **28**(2),pp.201–222.

KOPSTEIN, J. 2013. Metadata matters: how phone records and obsolete laws harm privacy and the free press. *The Verge* [online]. Available from: http://www.theverge.com/2013/5/16/4336994/metadata-matters-how-phone-records-and-obsolete-laws-harm-privacy [Accessed July 30, 2013].

KUKLOWSKY, C. 2011. Every Move You Make…. *Dr. Pop Blog* [online]. Available from: http://drpop.org/2011/04/every-move-you-make/ [Accessed July 13, 2013].

KUPERMAN, A.J. 2001. *The limits of humanitarian intervention: genocide in Rwanda*. Washington, D.C.: Brookings Institution Press.

LACKEY, D.P. 1988. *The Ethics of War and Peace* Facsimile. Prentice-Hall.

LANGO, J. 2006. Last Resort and Coercive Threats: Relating a Just War Principle to a Military Practice Available from: http://isme.tamu.edu/JSCOPE06/Lango06.pdf [Accessed June 14, 2013].

LAWLOR, R. 2006. Luck, Evidence and War. *Journal of Applied Philosophy*. **23**(3),pp.247–57.

LAWRENCE, F. 2010. First goal of David Cameron's 'nudge unit' is to encourage healthy living. *The Guardian* [online]. Available from:

http://www.guardian.co.uk/politics/2010/nov/12/david-cameron-nudge-unit [Accessed February 15, 2013].

LEE, M. 2012. Free Software Supporter: the Free Software Foundation's monthly news digest and action update. Available from: http://www.fsf.org/free-software-supporter/2012/april.

LOCKE, J.L. 2010. *Eavesdropping: An Intimate History*. OUP Oxford.

LOMELL, H.M. 2012. Punishing the Uncommitted Crime: Prevention, pre-emption, precaution and the transformation of criminal law *In*: B. HUDSON and S. UGELVIK, eds. *Justice and Security in the 21st Century: Risks, rights and the rule of law*. Oxford: Routledge, pp. 83–100.

LORD, S.M. 2010. *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway but Opportunities Exist to Strengthen Validation and Address Operational Challenges* [online]. Government Accountability Office. Available from: http://www.gao.gov/new.items/d10763.pdf [Accessed January 18, 2011].

LUDLOW, D.R.L. 1999. Humanitarian Intervention and the Rwandan Genocide. *Journal of Conflict Studies* [online]. **19**(1). Available from: http://journals.hil.unb.ca/index.php/JCS/article/view/4378 [Accessed August 2, 2013].

LYNCH, D. 1980. *The Elephant Man [DVD]*. Optimum Home Entertainment.

LYON, D. 2001. Facing the Future: Seeking Ethics for Everyday Surveillance. *Ethics and Information Technology*. **3**,pp.171–181.

LYON, D. 2002. Surveillance as Social Sorting: Computer Codes and Mobile Bodies *In*: D. LYON, ed. *Surveillance as Social Sorting*. Oxford: Routledge.

MACNISH, K. 2012. Unblinking eyes: the ethics of automating surveillance. *Ethics and Information Technology*. **14**(2),pp.151–167.

MARKOFF, J. 2002. Pentagon Plans a Computer System That Would Peek at Personal Data of Americans. *The New York Times* [online]. Available from: http://www.nytimes.com/2002/11/09/politics/09COMP.html [Accessed July 30, 2013].

MARX, G.T. 1998. Ethics for the New Surveillance. *The Information Society*. **14**,pp.171–185.

MAVRODES, G., I. 1975. Conventions and the Morality of War. *Philosophy and Public Affairs*. **4**(2),pp.117–131.

MCCAHILL, M. and C NORRIS 2003. Estimating the extent, sophistication and legality of CCTV in London *In*: M GILL, ed. *CCTV*. Palgrave Macmillan.

MCMAHAN, J. 2009. Intention, Permissibility, Terrorism, and War. *Philosophical Perspectives*. **23**(1),pp.345–372.

MCMAHAN, J. 2005. Just Cause for War. *Ethics and International Affairs*. **19**(3),pp.1–21.

MCMAHAN, J. 2006. Liability and Collective Identity: A Response to Walzer. *Philosophia*. **34**,pp.13–17.

MCMAHAN, J. 2007. The Sources and Status of Just War Principles. *Journal of Military Ethics*. **6**(2),pp.91–106.

MCSMITH, A. 2010. First Obama, now Cameron embraces 'nudge theory'. *The Independent* [online]. Available from: http://www.independent.co.uk/news/uk/politics/first-obama-now-cameron-embraces-nudge-theory-2050127.html [Accessed February 15, 2013].

MICA, J.L. 2010. Letter to Janet Napolitano, Secretary, Department of Homeland Security. Available from: http://republicans.transportation.house.gov/Media/file/111th/Aviation/2010-05-20-TSA_Reorg_Letter.pdf [Accessed January 18, 2011].

MILL, J.S. 1993. *Utilitarianism, On Liberty, Considerations on Representative Government* New edition. Phoenix.

NAGEL, T. 2012. *Mortal questions*. Cambridge; New York: Cambridge University Press.

NAGEL, T. 1972. War and Massacre. *Philosophy and Public Affairs*. **1**(2),pp.123–44.

NATHAN, D. 1990. Just looking: Voyeurism and the grounds of privacy. *Public Affairs Quarterly*. **4**(4),pp.365–386.

NATIONAL CONFERENCE OF CATHOLIC BISHOPS 2006. A Presumption Against War *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 670–682.

NAVARRO, J. 2012. What the Shoulders Say About Us. Available from: http://www.psychologytoday.com/blog/spycatcher/201205/what-the-shoulders-say-about-us [Accessed June 22, 2013].

NEGROPONTE, N. 1995. *Being Digital* 1st Vintage Ed. Vintage Books.

NIETZSCHE, F. and R.J. HOLLINGDALE 2005. *A Nietzsche Reader* Reprint. Longman.

NISSENBAUM, H. 2004. Privacy as Contextual Integrity. *Washington Law Review* [online]. **79**(1). Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=534622 [Accessed January 16, 2012].

NORRIS, Clive and G. ARMSTRONG 1999. *The Maximum Surveillance Society: The Rise of CCTV* First. Berg Publishers.

NOZICK, R. 2001. *Anarchy, State and Utopia* New Ed. Wiley-Blackwell.

O'DONOVAN, O. 2003. *The Just War Revisited*. Cambridge University Press.

O'HAGAN, E.M. 2012. A life under surveillance. *the Guardian* [online]. Available from: http://www.guardian.co.uk/commentisfree/2012/nov/01/unhappy-fact-activist-life [Accessed February 2, 2013].

O'NEILL, O. 1985. Between Consenting Adults. *Philosophy and Public Affairs*. **14**(3),pp.252–277.

O'NEILL, O. 1984. Paternalism and Partial Autonomy. *Journal of Medical Ethics*. (10),pp.173–178.

OREND, B. 2005. Is There a Supreme Emergency Exception? *In*: M. EVANS, ed. *Just War Theory: A Reappraisal*. Edinburgh: Edinburgh University Press.

OREND, B. 2000. *Michael Walzer on War and Justice*. University of Wales Press.

ORWELL, G. 2004. *1984 Nineteen Eighty-Four* New Ed. London: Penguin Classics.

OZ, F. 1986. *Little Shop of Horrors*.

PACE 1984. *Police and Criminal Evidence Act*.

PARENT, W.A. 1983. Privacy, Morality and the Law. *Philosophy and Public Affairs*. **12**(4),pp.269–288.

PENAFORT, R. 2006. Summa de Casibus poenitentiae, II *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 134–147.

PFANNER, T. 2004. Military Uniforms and the Law of War. *International Review of the Red Cross*. **86**(853),pp.93–124.

PICKLES, N. 2011. Nine in Ten TFL CCTV cameras fail to solve a single crime | Big Brother Watch. Available from: http://www.bigbrotherwatch.org.uk/home/2011/12/ten-tfl-cctv-cameras-fail-solve.html [Accessed August 19, 2012].

PIZAN, C. de 2006. From The Book of Deeds of Arms and of Chivalry, pt. III, chaps. 7, 12-14, 17-18, 21, 23 *In*: *The Ethics of War*. Oxford: Blackwell Publishing, pp. 217–224.

PLATO 2007. *The Republic* 3rd ed. Penguin Classics.

RACHELS, J. 1975. Why Privacy is Important. *Philosophy and Public Affairs*. **4**(4),pp.323–333.

RAINE, S. 2009. Surveillance in a New Religious Movement: Scientology as a Case Study. *Religious Studies and Theology*. **28**(1),pp.63–94.

RAWLES, K. 2002. *Compensation in Radioactive Waste Management: Ethical issues in the treatment of host communities* [online]. UK: UK Nirex. Available from: http://www.nda.gov.uk/documents/upload/Compensation-in-Radioactive-Waste-Management-Ethical-issues-in-the-treatment-of-host-communities-May-2002.pdf [Accessed February 20, 2013].

RAWLS, J. 1999. *A Theory of Justice Rev (Paper)* Revised edition. Harvard University Press.

REEVE, T. 2012. Security seminar hears from CCTV commissioner about industry regulation. *SecurityNewsDesk.com* [online]. Available from: http://www.securitynewsdesk.com/2012/11/15/security-seminar-hears-from-cctv-commissioner-about-industry-regulation/ [Accessed February 15, 2013].

RIPA 2000. *Regulation of Investigatory Powers Act* [online]. Available from: http://www.legislation.gov.uk/ukpga/2000/23/data.pdf [Accessed June 14, 2013].

ROBERTS, A. 2012. Bionic Mannequins Spy on Shoppers to Boost Luxury Sales. *BusinessWeek: undefined* [online]. Available from: http://www.businessweek.com/news/2012-11-19/bionic-mannequins-spy-on-shoppers-to-boost-luxury-sales [Accessed May 17, 2013].

ROSS, D. 2002. *The Right and the Good* New edition. (P. Stratton-Lake, ed.). Clarendon Press.

RYBERG, J. 2007. Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs Aremac. *Res Publica*. **13**(2),pp.127–143.

SANDELSON, M. 2013. People suffering from dementia could be tagged / News / The Foreigner. *the Foreigner: Norwegian News in English* [online]. Available from: http://theforeigner.no/pages/news/people-suffering-from-dementia-could-be-tagged/ [Accessed February 16, 2013].

SAVULESCU, J. 1995. Rational non-interventional paternalism: why doctors ought to makejudgments of what is best for their patients. *Journal of Medical Ethics*. **21**,pp.327–337.

SCANLON, T.M. 2008. *Moral Dimensions: Permissibility, Meaning, Blame*. Harvard University Press.

SCANLON, T.M. 1975. Thomson on Privacy. *Philosophy and Public Affairs*. **4**(4),pp.315–322.

SCOTT, T. 1998. *Enemy of the State*. Touchstone Pictures.

SELLGREN, K. 2010. Baby P ‘failed by all agencies’. *BBC* [online]. Available from: http://www.bbc.co.uk/news/education-11621391 [Accessed July 26, 2013].

SEWELL, G. and J.R. BARKER 2001. Neither Good, Nor Bad, But Dangerous: Surveillance as an Ethical Paradox. *Ethics and Information Technology*. **3**,pp.183–196.

SIMPSON, E. 2006. Chechen war reporter found dead. *BBC* [online]. Available from: http://news.bbc.co.uk/1/hi/world/europe/5416218.stm [Accessed July 29, 2013].

SLACK, J. 2010. How town hall snoopers are watching you: Councils use anti-terror laws to spy on charity shops and dog-walkers. *Mail Online* [online]. Available from: http://www.dailymail.co.uk/news/article-1280672/How-town-hall-snoopers-watching-Councils-use-anti-terror-laws-spy-charity-shops-dog-walkers.html [Accessed February 2, 2013].

STEWART, W. 2010. Secret documents confirm Stalin DID sanction Katyn massacre... but Russia still won't name police who shot 22,000. *Mail Online* [online]. Available from: http://www.dailymail.co.uk/news/article-1269550/Russia-releases-documents-signed-Stalin-ordering-Katyn-massacre.html [Accessed August 19, 2012].

STRUHL, K.J. 2005. Is War a Morally Legitimate Response to Terrorism? *The Philosophical Forum*. **36**(1),pp.129–137.

TAVANI, H.T. and J.H. MOOR 2001. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *Computers and Society*. **31**(1),pp.6–11.

THALER, R.H. and C.R. SUNSTEIN 2009. *Nudge: Improving Decisions About Health, Wealth and Happiness*. Penguin.

THOMSON, J.J. 1992. *The Realm of Rights* New Ed. Harvard University Press.

THOMSON, J.J. 1975. The Right to Privacy. *Philosophy and Public Affairs*. **4**(4),pp.295–314.

TONER, C. 2010. The Logical Structure of Just War Theory. *Journal of Ethics*. **14**(2),pp.81–102.

UNITED NATIONS 2013. Background Information on the Responsibility to Protect — Outreach Programme on the Rwanda Genocide and the United Nations. *Background Information on the Responsibility to Protect* [online]. Available from: http://www.un.org/en/preventgenocide/rwanda/about/bgresponsibility.shtml [Accessed August 2, 2013].

UNITED NATIONS 1945. Charter of the United Nations. Available from: http://www.un.org/en/documents/charter/chapter7.shtml [Accessed June 21, 2013].

UNITED NATIONS 1948. The Universal Declaration of Human Rights. Available from: http://www.un.org/en/documents/udhr/index.shtml [Accessed June 13, 2011].

US SUPREME COURT 1942. *Ex Parte Quirin - 317 U.S. 1* [online]. Available from: https://supreme.justia.com/cases/federal/us/317/1/case.html [Accessed July 6, 2013].

DE VATTEL, E. 2006. From The Law of Nations *In*: *The Ethics of War*. Oxford: Blackwell Publishing, pp. 506–17.

VITORIA, F. de 2006. On the Law of War *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 324–332.

WALZER, M. 2004. *Arguing About War*. New Haven, Conn.: Yale University Press.

WALZER, M. 2006a. *Just and Unjust Wars: A Moral Argument with Historical Illustrations* Revised edition. Basic Books.

WALZER, M. 2007. Response. *Journal of Military Ethics*. **6**(2),pp.168–71.

WALZER, M. 2006b. Response to Jeff McMahan. *Philosophia*. **34**,pp.19–21.

WEIR, P. 1998. *The Truman Show*.

WINNER, L. 1977. *Autonomous Technology: Technics-out-of-control as a Theme for Political Thought*. The MIT Press.

VON WOLFF, C. 2006. From The Law of Nations Treated according to a Scientific Method *In*: G. M. REICHBERG, H. SYSE and E. BEGBY, eds. *The Ethics of War*. Oxford: Blackwell Publishing, pp. 470–74.