Ph.D. THESIS

Ethics of Lifelog Technology

By Tim Jacquemard, B.A., M.A.

School of Computing

Supervisors:

Prof. Bert Gordijn

Prof. Alan F. Smeaton

September, 2014

Dublin City University

Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Ph.D. is entirely my own work, that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: ID No.:   Date:

Acknowledgements

As I have come to see, a Ph.D. is never the work of one person, but the result of the combined efforts of many. Firstly, I am thankful to my supervisors, Alan and Bert, for their guidance and feedback throughout the process. Special thanks to Bart, Elizabeth, Fiachra, Jurjen, Peter, Renaat, and Wouter for their invaluable contributions as editors and/or technical support. Lastly, I would like to show my warm gratitude to Louise, my parents, my sister, my family and friends in Dublin, the Netherlands, and beyond. I am incredibly fortunate to have such a loving and supportive environment.

Contents

Abstract

In a lifelog, data from different digital sources are combined and processed to form a unified multimedia archive containing information about the quotidian activities of an individual. This dissertation aims to contribute to a responsible development of lifelog technology used by members of the general public for private reasons.

Lifelog technology can benefit, but also harm lifeloggers and their social environment. The guiding idea behind this dissertation is that if the ethical challenges can be met and the opportunities realised, the conditions will be optimised for a responsible development and application of the technology. To achieve this, it is important to reflect on these concerns at an early stage of development before the existing rudimentary forms of lifelogs develop into more sophisticated devices with a broad societal application. For this research, a normative framework based on *prima facie* principles is used.

Lifelog technology in its current form is a relatively novel invention and a consensus about its definition is still missing. Therefore the author aims to clarify the characteristics of lifelog technology. Next, the ethical challenges and opportunities of lifelogs are analysed, as they have been discussed in the scholarly literature on the ethics of lifelog technology.

Against this backdrop, ethical challenges and opportunities are identified and elaborated. The normative analysis concentrates on two areas of concern, namely (1) the ethical challenges and opportunities that result from the use of lifelog technology, and (2) the conditions under which one becomes a lifelogger. For the first, three sets of key issues are discussed, namely issues to do with (a) privacy, (b) autonomy, and (c) beneficence. For the second, one key set of issues is examined, namely issues to do with autonomy. The discussion of each set of issues is concluded with recommendations designed to tackle the challenges and realise the opportunities.

List of Tables

List of Figures

List of Appendices

1 Introduction

Introduction

Already many people are using different kinds of devices that can be used to create digital information about their daily activities. In addition, many of these devices are able to spread these data throughout networks. Indeed, it is unlikely that you would be reading this on a computing device which does not have both integrated sensors *and* network connectivity. The proliferation of sensors and networking technology are fundamental enablers for the idea that we should aim to capture everything we possibly can from the physical world. This idea is embodied by the term 'Sensor Web'. The idea behind the Sensor Web is that "…every second of every day, information is created through naturally occurring events in the physical world but these events go largely unnoticed and the information is lost. In the world of the Sensor Web this is set to change" (Smyth 2009). In the Sensor Web, information about the physical world is as readily available as information about events that happen digitally. However, the work in this dissertation is restricted to a specific technology developed to capture that part of the Sensor Web that concerns individuals, namely lifelog technology. If the notion of the Sensor Web embodies the aim to retrieve digital information about anything whatsoever in the physical world, lifelogs embody the aim to do just that for individual human beings. Cathal Gurrin, a prolific auto-experimenter in the field of lifelog technology, aptly called a lifelog a "search engine for the self" (The Economist 2014). Having the individual as its locus, lifelog technology will most likely have a tremendous impact on the lives of individuals and society in general.

1.1 Research question

The main objective of this dissertation is to contribute to optimising a responsible development of lifelog technology. Lifelog technology is still at an early stage of development: few devices and applications have yet been developed for this purpose and the ability to search for personal information within a lifelog is likely to improve significantly. Within this research, challenges - challenges are interpreted as potential undesirable moral consequences resulting from the development and use of the technology – and opportunities - opportunities are interpreted as potential desirable moral consequences resulting from the development and use of lifelog technology – are identified. The idea is that the identification of challenges and opportunities inform approaches that aim to meet the challenges and realise

the opportunities, so that the technology is beneficial for or, at least, does minimal to no harm to the interests of lifeloggers and non-lifeloggers.

The inquiry is restricted in eight important ways.

1) The moral challenges and opportunities manifest at three different stages: research and development, trials, and use. The analysis at hand focuses on challenges and opportunities that occur when lifelog technology is available and used as an end-product.

2) Lifelog technology can be used by different agents: private individuals, public institutions, government agencies, and corporations could deploy lifelog technology. This study is concentrated upon lifelog technology that is purchased or installed by members of the general public.

3) Lifelog technology can be used for different purposes. In this study, the use of lifelogs for private purposes by members of the general public is discussed. As shown later (*2.3.2 Purposes* and *2.3.3 Users*), lifelog technology can also be deployed in professional or medical settings, so that a better insight into the behaviour of employees or patients is obtained.

4) Even more specifically, when lifelog technology is made available to members of the general public, the moral challenges and opportunities manifest at three stages: (1) when a non-lifelogger becomes a lifelogger; (2) when lifelogs are being used; (3) and when a lifelogger quits being a lifelogger. This study focuses on the first two.

5) Lifelogs are currently only at a rudimentary stage of development, leaving room for a broad spectrum of contingencies concerning their future functioning. Therefore, a plausible future scenario is used to delimit ethical research and illustrate ethical concerns. Since the technology is still at an early stage of development, a future scenario is generally an acceptable way to contextualise the ethical analysis and identify normative issues (Wright et al. 2008). The scenario is not intended to be an accurate prediction of the future. Instead it provides one of many future possibilities, which can be used to discuss the potential merits and demerits of the technology. Even though the scenario is fictional, the plausibility of the scenario will be substantiated by referring to current research findings.

6) This research focuses on three key sets of issues, namely issues with respect to privacy, autonomy, and beneficence, when discussing the moral challenges and opportunities

that manifest when lifelogs are being used. In the literature review conducted for this research, these three sets of issues are shown to be key sets of issues that need further exploration. For the discussion on the conditions in which one becomes a lifelogger, the inquiry is focused on a set of issues related to autonomy.

7) Although existing regulation relevant to lifelog technology is important, e.g. when it sets limits to information flows, this research focuses on the ethical aspects of lifelog technology rather than on legal issues. One reason to refrain from providing a systematic analysis of existing legal frameworks is that there currently are great differences in regulation between jurisdictions. As lifelog technology is not confined to one jurisdiction, but is likely to proliferate, and lifelog products and services, such as data servers, can be offered from any suitable geographical location, a thorough examination of all existing regulation would be beyond the reach of this study. In addition, the findings of this research may inform the development of robust national or international regulation that can account for ethical challenges and opportunities posed by lifelog technology rather than use these regulations as a given. After all, existing legal frameworks for lifelog technologies are not necessarily ethical.

8) This research aims to provide design recommendations instead of recommendations for regulation or a responsible use of lifelog technology. Early identification and adjustments during research and development prevent costly measures to correct harm and achieve benefits at later stages. In addition, addressing issues at later stages may be more difficult when the technology has already become widely used.

1.2   Relevance
The identification of challenges and opportunities is supposed to inform a 'value sensitive design'- approach in which the design of lifelogs could be adjusted so as to meet the challenges and reap the opportunities in order to guide an ethically responsible development of lifelog technology (for example see Friedman (1996) and Flanagan, Howe, and Nissenbaum (2008) for 'value sensitive design'-approaches).

It is imperative to discuss technology at an early stage of development rather than at a stage in which its form and uses have already solidified. Ethical reflection might still influence the development of a technology at an early stage of its development whereas this becomes more difficult when it has become commonplace (Collingridge 1980). An inquiry is

justified because specific technologies can have idiosyncratic effects, which can be felt by an individual (Borgmann 1984; Idhe 2002), on a societal (Bijker 1995; Latour 2005) and political (Winner 1986) level and lifelogs do have the potential to trigger distinctive ethical concerns as they enable the storage and access of an unprecedented amount of personal information about lifeloggers and their environment. An early identification of the opportunities and challenges created by lifelog technology might prevent harm caused by unsound technology to the interests of lifeloggers and society in general.

Identification of issues at this stage of development also has ramifications for the development of the field and the adoption of lifelog technology. Failures to comply with ethical demands do not just signify a denial of a developer's moral responsibility to their users and to society at large, but they could also harm the interests of the field of lifelog technology. The irresponsible proliferation of lifelog technology could create a popular backlash against the technology hurting investments and developments. In addition, identifying issues at an early stage prevents time and other resources being invested in technology that lacks societal support.

There are many ethical challenges and opportunities expected from lifelog technology. This dissertation attempts to provide instruments to meet these challenges and realise these opportunities. The literature review (*3.2 Results*) reveals the existence of a rich debate on the ethics of lifelog technology. Nonetheless, many challenges and opportunities have yet to be discussed or, when already identified, require further elaboration. Privacy, for example, has been mentioned as a concern for lifelog technology in half the sources used for the literature review, but a comprehensive overview of all issues associated with privacy and lifelog technology seems to be missing.[1] Moreover, recommendations for lifelog technology are offered that can be applied to a wide range of lifelog devices and applications; such recommendations have not been provided in the current academic debate as revealed in this research.

1.3 Methodology
After explaining the properties ascribed to lifelog technology and the existing scholarly debate on the ethics lifelog technology, a normative analysis of lifelog technology is

---

[1] Only Lahlou (2008) has aimed to provide a comprehensive overview of concerns for privacy and to offer recommendations, but he focused on one kind of lifelog technology, which limited the reach of his research.

provided. The next section details the underlying normative framework in which the issues are discussed.

There are three strands of ethics, namely descriptive, normative and meta-ethics (Frankena 1973). Descriptive ethics is an empirical, historical or scientific inquiry of moral phenomena. This is mostly the work of sociologists, historians, anthropologists, and psychologists. Descriptive ethics might, for example question how the value of freedom is *de facto* perceived or how people *de facto* deal with privacy. Meta-ethics discusses fundamental questions about the nature of normative judgements. Normative ethics does not describe how people in fact act or think, but prescribes how they ought to act and think. It endeavours to argue in favour of a particular view on what is intrinsically good, one's duties and/or one's virtues. This dissertation contains a normative analysis of lifelog technology.

A deontological approach is used, which means that the standard for right or wrong is not primarily determined by the perceived or actual consequences of actions but by adherence to one or more rules. More specifically, elements of different ethical theories are combined in the normative framework used in this study, namely theories of William D. Ross, Richard Brandt, Thomas Beauchamp and James Childress: Ross' distinction between *prima facie* and *actual* duties is advanced to describe the functioning of principles in particular circumstances; Brandt's theory of deliberation and the mid-level principles of Beauchamp and Childress are put forward to complement Ross' original framework for moral decision-making.

1.3.1 Consequentialism

A few issues associated with consequentialism are discussed first, without claiming to be exhaustive, to explain the choice for deontology in the study at hand rather than a consequentialist approach. According to consequentialism the moral rightness of an act depends entirely on the consequences (Sinnott-Armstrong 2011). Utilitarianism is the best known consequentialist theory. Its main proponents were Jeremy Bentham (1907), John Stuart Mill (1879), and Henry Sidgwick (1877). Peter Singer (1972) is a contemporary philosopher in the tradition of utilitarianism. The good that is ascribed intrinsic worth as used by different consequentialist theories can vary. Things such as pleasure, happiness, desire satisfaction, knowledge, power, virtue, or combinations have been considered as intrinsically valuable by various ethicists.

There are several objections advanced against consequentialism. Firstly, predicting consequences is notoriously difficult. The number of people affected might be manifold and their exact number and the degree in which they are affected can be unclear. The balancing of good over evil is particularly troublesome when the good that is to be weighed is a mental state, such as happiness, which would require measuring the happiness of one person against the happiness or unhappiness of others. Secondly, the outcomes are sometimes contrary to commonly held moral intuitions. Hedonistic interpretations of consequentialism could prescribe, for instance, sadistic behaviour that one would ordinarily find immoral. After all, if this behaviour leads to the greatest amount of pleasure for the greatest number of people, then it can be considered ethically desirable. Furthermore, according to Frankena (1973), many actions that seem to be and are commonly regarded as wrong can be justified based on consequentialist outcomes – e.g. the poor man who steals a loaf of bread from a wealthy family to save his own family from starvation – and sometimes rightly so. However, consequentialism allows too many cases of stealing, cheating, lying, *et cetera*, than what we would ordinarily consider acceptable. Thirdly, consequentialism could fail to provide intrinsic value to things one would ordinarily consider of value. Nozick (1974) formulated a thought experiment, namely the Experience Machine. This machine fabricates desirable experiences that are indistinguishable from non-fabricated experiences. Hence, one could experience the fulfilments of desire because of the fabrications of the machine, but in reality one may have achieved nothing. When the machine would be superior in optimising happiness in the form of pleasure and the absence of pain, hedonists should choose the experience machine above actual achievements. However, commonly held moral intuitions lead one to believe that certain benefits should not only be felt but also be real, e.g. friendship should not only be perceived but people generally want to actually have friends. Authenticity seems to be valued as well besides pleasure. Fourthly, consequentialism may fail to attach proper weight to the principle of justice. Frankena (1973) states that the distribution of the balance of good over evil can be unjust. In case all the good is randomly, without good reason, allocated to a small group of people, while the risks are spread out over a large group of people, a distribution might be preferred with a smaller sum of good spread more evenly. Hence, a pure consequentialist approach seems to yield unsatisfactory results.

1.3.2 Deontology

In contrast to the above, deontological theories assert that there are considerations that make an action or rule right or wrong other than its perceived or actual consequences.

Deontological theories shy away from theories that determine the morality of actions exclusively by their consequences. Regardless how good the consequences are, some choices are simply impermissible (Alexander & Moore 2012). Some deontological theories hold that moral obligations ultimately derive from God's commands. Others consider moral principles to be founded in practical reason. Arguably one of the most influential deontologists was Immanuel Kant who asserted that one should always treat others as an end and never solely as a means to an end, which is underlying the conception of human dignity as it appears in the Universal Declaration of Human Rights (United Nations 2013). The justification, content, and number of moral principles differ between different deontological theories. Kant has one fundamental moral principle, which functions at a high level of abstraction. In contrast, Ross (2002) holds multiple moral principles.

1.3.3 *Prima facie principles*

Ross' idea of *prima facie* principle is used throughout this study. Ross holds that there is not one unifying principle but that there can be multiple principles at play in a particular context. He regards the idea of only one guiding principle as an oversimplification of moral life and contrary to how ethics are used in daily life (Ross 2002, 23-24).

Ross aims to both acknowledge the complexity of ethical decision-making while avoiding conflicting duties to act. In order to achieve this, he distinguishes between *prima facie* duties and *actual* duties. *Prima facie* duties constitute valid moral considerations in favour of a particular course of action whose strength can only be determined within a particular situation. He distinguished 6 *prima facie* duties, namely 1a) fidelity, 1b) reparation, 2) gratitude, 3) justice, 4) beneficence, 5) self-improvement and 6) non-maleficence (Ross 2002, 21-22).[2] According to Ross, in any moral situation where *prima facie* duties conflict with each other only one duty is decisive. This dominant *prima facie* duty then becomes the *actual* duty. Hence, although the *prima facie* duties are always valid considerations, there is no conflict at the level of execution. According to Ross, an action is both *prima facie* wrong and right in case two or more *prima facie* duties conflict (Ross 2002, 34). For instance, sometimes a lie is required to prevent harm from occurring. The principle of fidelity provides a *prima facie* obligation to be honest while at the same time the principle of non-maleficence provides a *prima facie* obligation not to do harm. However, only one obligation can be decisive. So one has to balance the *prima facie* obligations and choose the dominant one

---

[2] Ross lists the first duty as consisting of separate parts, namely as 1a and 1b. The first duty may be interpreted as two separate duties.

depending on the characteristics of the particular situation. Ross proposes to use intuition for the weighing of *prima facie* obligations. He does not provide a rigid order of priority to solve conflicts.

Consequentialist considerations have a place for Ross as well. By deploying the principles of beneficence and non-maleficence Ross can take the outcomes of actions into account. The principles of beneficence and non-maleficence have weight in situations in which harm or benefit seem relevant. However, Ross avoids his theory becoming too demanding, i.e. that one continuously has to maximise outcome for every act, as the principles of beneficence and non-maleficence can be balanced out by other principles.

The idea that a moral situation incites conflicting principles seems well suited when discussing technology. It is quite evident that most technology has good and bad characteristics. Using *prima facie* duties the complexity of a technology can be fully accounted for without the need to simplify these issues to suit the parameters of a monistic theory. In addition, discussing technology using widely-carried principles, such as respect for privacy and respect for autonomy, has a rhetorical advantage as the importance of these principles is widely accepted.

Ross is an intuitionist in the tradition of H.A. Prichard and Henry Sidgwick. He is influenced by Aristotle from whom he even borrows the phrase: "the decision rests with perception" (Ross 2002, 42). Ross hints that every moral decision triggers some conflict between *prima facie* duties, as he states: "[moral acts] always … have different characteristics that tend to make them at the same time *prima facie* right and *prima facie* wrong" (Ross 2002, 33). To solve these dilemmas one has to reflect on one's intuitions. One of the main concerns with Ross' intuitionist account is that the scope left for discussion is very limited. According to him is "that to make a promise, for instance, is to create a moral claim on us in someone else. Many readers will perhaps say that they do *not* know this to be true. If so, I certainly cannot prove it to them; I can only ask them to reflect again, in the hope that they will ultimately agree that they also know it to be true" (Ross 2002, 21).[3] The scope for intersubjectivity is widened using Brandt's concept of attitudes (see below).

---

[3] He also defends his list of *prima facie* duties on the same grounds. The lack of system does not make the identified duties arbitrary as "[t]he list of goods put forward by rival theory is reached by exactly the same method – the only sound one in the circumstances – viz. that of direct reflection on what we really think. Loyalty to the facts is worth more than a symmetric architectonic or a hastily reached simplicity" (Ross 2002, 23).

1.3.4 Scope for intersubjectivity

Ross' concept of intuition leaves little scope for discussion as one could only request the other to reflect on their intuitions. Brandt provides further insight into the conditions that arguments have to meet in order to not be refused and/or have some power of persuasion. One can criticise the outcome of ethical reflections by judging arguments based on these conditions.

Brandt's account for the weighing of principles is more convincing and elaborate than the one of Ross. Using principles for ethical analysis is not straightforward: principles can conflict; they might leave scope for interpretation; and sometimes they have to be corrected or even abandoned (Brandt 1959, 246-247). In order to solve conflicts between principles and to correct them, if necessary, one needs to be able to refer to an additional entity besides principles. According to Brandt, one should use one's attitudes to perform these critical operations (Brandt 1959, 246). People have attitudes towards moral issues, e.g. feelings of obligation, feelings of guilt, impulses, emotions, preferences (Brandt 1959, 206 and 246). However, these attitudes are not unconditionally acceptable as ethical guides, e.g. one can feel guilty for things which one should not feel guilty for. Therefore attitudes need to meet certain conditions in order not to be discounted (Brandt 1959, 209). Brandt stipulates four conditions for an attitude to be discounted: (1) partiality[4]; (2) insufficient understanding; (3) an abnormal state of mind; and (4) it evokes a group of principles too complex to serve as a guide for conduct to oneself or others and does not allow explicit statements, i.e. this requirement more or less entails that the principles evoked should be practical, consistent and general (Brandt 1959, 249-250). Suppose person 'A' feels guilty because she is misinformed about the situation, you or someone else could question and discount her attitude by pointing out to her that her moral attitude is based on false information. Brandt's account aligns well with how one would deliberate on moral issues in daily life. More importantly, the possibilities to critically assess the conditions under which normative statements are made allow the ethical debate to further develop.[5]

---

[4] Impartiality is not the being of ideal observer, or someone who does not hold particular moral views. Instead Brandt seems to suggest that an attitude would not be discounted if it would not change if the roles do change (Brandt 1959, 249).

[5] Thus ethical views and assessments are amenable to a variety of rational criticisms. For example, a set of principles is inconsistent; principles contain unintelligible notions; the outcome is the result of partiality; there was a misunderstanding; the result of the application of principles is unclear; the principles do not support the decision (Brandt 1959, 299-300).

1.3.5 Mid-level principles

Beauchamp and Childress have developed arguably the most influential approach within the discipline of bioethics. Their approach can be labelled 'principlism' (Bulger 2009). Bioethics is a relatively new field of ethics. The term was established in the 1970s although some of its topic can be traced back as far as the Hippocratic Oath (500 BCE) or even to the Code of Hammurabi (1750 BCE) (Gordon 2012). Principlism or versions of principlism have been proposed and defended by numerous authors (Bulger 2009; DeGrazia 1992; Gordon 2011; Lustig 1992; Richardson 1990).

Beauchamp and Childress have advanced the idea of mid-level principles. Theoretically the justification of principles can be provided top-down, bottom-up or by a coherence-theory (Beauchamp & Childress 2009, 369, and 381). Beauchamp and Childress prefer the latter method. A top-down approach uses deduction; universal precepts have to be applied to the relevant facts, which are deduced from an abstract ethical theory, such as Kantianism or utilitarianism. Top-down approaches all seem to suffer from one or more of the following difficulties according to Beauchamp and Childress (2009, 369-371). The principles deployed can be so general that they fail to provide clear instructions to determine moral obligations. Furthermore, the principles can be internally inconsistent and may provide contradicting duties to act.[6] In addition, the justification of the principles may be unsatisfactory as it often leads to infinite regress as their most general principles need justification, and that justification needs justification, *et cetera*. Finally, there is no general consensus on which ethical theory to use. Bottom-up approaches are, in contrast, inductive and consider moral principles to arise from daily practice (Beauchamp & Childress 2009, 376). For example, casuistry states that moral judgements are often made without universal moral principles and that one uses precedents and paradigms to guide one's conduct rather than moral theories. However, there are several problems associated with casuistry related to the lack moral premises; paradigm cases are not self-evident but need moral explanations; paradigm cases can be prejudiced or poor; and analogies often fail (Beauchamp & Childress 2009, 379-380).

Against the backdrop of the failings of both top-down and bottom-up approaches Beauchamp and Childress prefer a position in the middle; although one does not need an abstract, top-down theory to start with, one does need moral principles in order to advance

---

[6] *Prima facie* principles may conflict but there is no conflict at the level of actual obligations.

substantiated ethical assessments. These are the so-called mid-level principles. According to Beauchamp and Childress one can distinguish 'common morality', which holds universal values shared by individuals and communities with a commitment to morality, from 'particular moralities', which are particular to individuals, cultures and groups. The common morality contains established and unbiased moral beliefs, such as the two universally shared principles that one ought not to murder and one ought not to steal. Beauchamp and Childress identify four mid-level principles, autonomy, non-maleficence, beneficence and justice, which all belong to the common morality. These principles are content-thin. For this reason, they need to be specified in order to be applied to a particular situation (Beauchamp & Childress 2009, 16-17). The specifications are part of the particular moralities. However, this is not idiosyncratic to mid-level principles. Theoretically, moral rules are always subject to specification as the complexity of reality is too difficult to be captured in general norms (Beauchamp & Childress 2009, 18).

The generality of mid-level principles allows different and possibly conflicting specifications (Beauchamp & Childress 2009, 388). The operation of the principles and thus the specification of principles will take place using Brandt's notion of attitudes. The set of principles from the common morality as used in the current study will be open and will include principles of respect for autonomy, beneficence, and privacy. In contrast to Beauchamp and Childress, respect for privacy is considered a mid-level principle. The specific set of principles by Beauchamp and Childress is developed for bioethics. Bioethics can broadly be described as the ethical reflection on issues in medicine, the biomedical, life and environmental sciences. However, the subject matter of this dissertation is technology. Therefore an open set of principles will be used, which provides the necessary scope to include additional principles, so as to be able to adequately address the ethical intricacies of technological developments.

1.3.6 Ethical assessment

There is a distinction between *prima facie* and actual duties. So one can have multiple valid obligations, but only one outweighs the others in a particular situation. Ross' theory of intuition to balance principles seemed insufficient. Hence, it was necessary to add another element to provide a better procedure for moral choice. Therefore, the theory of deliberation as described by Brandt has been advanced to clarify the way one selects, balances, specifies and modifies principles and chooses the decisive principle in a particular situation. Moreover,

the idea of mid-level principles as furthered by Beauchamp and Childress clarifies the nature of the chosen principles. Also, since the set of principles as advanced by Beauchamp and Childress was insufficient to ethically assess technology, an open set of principles is used suitable to deal with ethical questions regarding technology.

Therefore, an ethical assessment in the study at hand proceeds as follows: an appeal is made both to the mid-level principles and attitudes. Attitudes are discounted if necessary. Next, the undiscounted attitudes are used to weigh the principles. If suitable, the principles are corrected, amended or abandoned. The methodology applied in this dissertation provides a rich understanding of the complexity of ethical decision-making. It makes the arguments in favour and against a certain course of action transparent. It thereby opens up the analysis for intersubjective criticism and rational debate.

1.4 Outline

This study into the ethics of lifelog technology begins with an explanation of the technology (*2 The technology)*. The literature demonstrates a wide disparity in interpretations of lifelog technology. Lifelog technology is a relatively novel phenomenon, and a consensus about its definition and its properties has yet to occur in the academic debate. A working definition of lifelog technology is proposed in this research to delimit the concept from other technologies and offer more precision in the scholarly discussion. The concept of lifelog technology is further expanded by identifying properties, of which many have yet to be acknowledged in the current debate, namely: the purposes for which lifelogs can be used; the different users of lifelog technology; and the data sources suitable for lifelogging. In this section, one can also find a scenario, which sheds more light on the kind of lifelogs that are discussed in this study.

Next, a literature review discussing the scholarly debate on the ethics of lifelog technology is presented (*3 Literature Review)*. This literature review explains current ethical challenges and opportunities in the debate on the ethics of lifelogging as well as a critical reflection to identify challenges and opportunities that have been ignored. This research contains - as far as the author knows – the only comprehensive literature review on lifelog technology, despite the substantial interest shown in the topic, currently available in the academic discussion on the ethics of lifelogs. In order to obtain an expansive overview of the present discussion, the review contains a wide range of sources, such as books, articles, chapters and conference proceedings. It is hoped that the literature review will be a valuable starting point for those that aim to get a better understanding of the current academic debate

on the ethics of lifelog technology. The literature review contains four elements: (1) an overview of the challenges and opportunities already identified; (2) a time frame in which the sources used for the review were published; (3) a critical analysis identifying issues that are undeveloped or neglected; and (4) (indirectly) an insight into the scholars involved.

The normative analysis concentrates on two areas of concern, namely (1) the ethical challenges and opportunities that result from the use of lifelog technology for lifeloggers and non-lifeloggers, and (2) the conditions under which one becomes a lifelogger. For the first, three sets of key issues have been identified, namely issues to do with (a) privacy, (b) autonomy, and (c) beneficence. In addition to privacy, the literature review conducted within the framework of this dissertation demonstrated that the latter two concerns have been barely been identified or not at all. For the second, one key set of issues has been identified, namely issues to do with autonomy. This area of concern has largely been neglected within the discussion on the ethics of lifelog technology.

The first set of issues analysed relates to the privacy of lifeloggers and non-lifeloggers. Privacy has been a pivotal concern in the ethical debate on lifelog technology as exactly half of the sources discussed in the literature review mentioned privacy-related concerns.[7] It is the main objection brought forward with regard to lifelogs, although a comprehensive analysis of the issue is lacking and no generalisable recommendations are offered, that aim to cover most concerns. The analysis in this study aims to be the most complete analysis of the relation between lifelog technology and privacy to date. It shows a wide variety of concerns related to privacy. In addition, recommendations are provided to address the identified concerns. Finally, a checklist is provided as an appendix that can be used to identify potential privacy issues (*Appendix A: Checklist for privacy*).

This study also contains the first comprehensive discussion of autonomy and lifelog technology. The chapter on autonomy discusses the potential effect of the use of lifelog technology on the autonomy of lifeloggers and non-lifeloggers. Similar to privacy, in the chapter on autonomy, ethical challenges with regard to autonomy are explained. However, unlike with privacy, lifelog technology may actually have the potential to meaningfully benefit the autonomy of lifeloggers and non-lifeloggers. Both the opportunities as well as challenges to autonomy are examined. Recommendations to address the opportunities and

---

[7] But one of the sources (Lahlou 2008) has aimed to provide a comprehensive overview of concerns about privacy. However his use of geolocation as the backdrop to identifying privacy issues has limited the scope of his inquiry as lifelog technology can be much more extensive than geolocation.

challenges related to the autonomy of lifeloggers and non-lifeloggers conclude this chapter. An appendix containing a checklist is added (*Appendix B: Checklist for autonomy*) to identify possible ethical challenges and opportunities that lifelog technology potentially poses to autonomy.

A third set of issues relate to the proportionality of beneficial and detrimental effects of lifelogs. Beneficence is a *prima facie* principle to prevent evil and promote the good (Frankena 1973). In this section, the valuable ends that can be promoted with or hindered by lifelogs are identified. Piecemeal discussions of several aspects of the good, most notably health and emotions, have taken place in the current scholarly literature, but a comprehensive overview of beneficial and detrimental effects of lifelogs appeared to be lacking in the debate to date. Several ethical challenges and opportunities of lifelogs with regard to the good are examined. This chapter is concluded with recommendations to deal with these challenges and opportunities. Again, a checklist is provided as an appendix (*Appendix C: Checklist for beneficence*) to identify possible ethical challenges and opportunities lifelogs related to the good.

A fourth set of issues has likewise been neglected in the academic literature on the ethics of lifelogs as yet: namely autonomy-related concerns about the conditions under which one becomes a lifelogger. The sole indication of this issue in the current literature was superficial. This is the second chapter discussing autonomy-related concerns. However, the primary focus of this chapter is the conditions under which one becomes a lifelogger rather than the effects of using lifelogs on lifeloggers and non-lifeloggers. There are several challenges identified in this chapter that have yet to be mentioned in the literature. Similar to the three previous chapters, recommendations are offered and a checklist is offered in an appendix (*Appendix D: Checklist for becoming a lifelogger*).

In the conclusion, a short summary of the finding of the previous chapters is presented. Furthermore an outlook is provided for future avenues for research.

Bibliography

Alexander, L. & Moore, M. 2012. Deontological Ethics [Online]. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Winter 2012 Ed. Available from: http://plato.stanford.edu/archives/win2012/entries/ethics-deontological/ [Accessed 20-03-2013].

Allen, A.L. 2008. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74.

Beauchamp, T.L. & Childress, J.F. 2009. *Principles of Biomedical Ethics: Sixth Edition*. New York & Oxford: Oxford University Press.

Bentham, J. 1907. An Introduction into the Principles of Morals and Legislation. Oxford: Clarendon Press.

Bijker, W.E. 1995. *Of bicycles, bakelites, and bulbs: toward a theory of sociotechnical change*. Cambridge: MIT Press.

Borgmann, A. 1984. Technology and the character of contemporary life. Chicago & London: Chicago University Press.

Brandt, R.B. 1959. *Ethical Theory: The Problems of Normative and Critical Ethics.* Englewood Cliffs: Prentice-Hall, Inc.

Brandt, R.B. 1990. The Science of Man and Wide Reflective Equilibrium. *Ethics*, 100(2), pp. 259-278

Bulger, J.W. 2009. An Approach towards Applying Principlism. *Ethics & Medicine*, 25(2), pp. 121-125.

Collingridge, D. 1980. *The social control of technology*. New York: St. Martin.

DeGrazia, D. 1992. Moving Forward in Ethical Theory: Theories, Cases, and Specified Principlism. *Journal of Medicine and Philosophy* 17(5), pp. 511-539.

The Economist. 2013. A search engine for the self [Podcast]. Available from http://www.economist.com/blogs/babbage/2013/11/cathal-gurrin-life-logger# [Accessed 27-03-2014].

Flanagan, M., Howe, D.C., & Nissenbaum, H. 2008. Embodying Values in Technology: Theory and Practice. *IN:* Van den Hoven, J. & Weckert, J. (eds.) *Information technology and moral philosophy*. Cambridge: Cambridge University Press, pp. 301-321.

Frankena, W.K. 1973. *Ethics.* Englewood Cliffs: Prentice-Hall, Inc.

Friedman, B. 1996. Value-Sensitive Design. Magazine interactions, 3(6), pp. 16-23.

Gordon J.S. 2011. Global ethics and principlism. *Kennedy Inst Ethics J*, 21(3), pp. 251-76.

Gordon, J.S. 2012. Bioethics [Online]. *IN:* Frieser, J. & Dowden, B. *Internet Encyclopedia of Philosophy*. 2013. Available from: http://www.iep.utm.edu/bioethic/ [Accessed 21-03-2013].

Ihde, D. 2002. *Bodies in Technology*. Minneapolis: Minnesota University Press.

Kant, I. 1785. Fundamental Principle of the Metaphysic of Morals [Online], translated by Abbott, T.K. *Project Gutenberg* Available from: http://www.gutenberg.org/cache/epub/5682/pg5682.html [Accessed 04-10-2013].

Kant, I. 2003. *Critique of Practical Reason*. Translated by McGregor, M. Cambridge: Cambridge University Press.

Lahlou, S. 2008. Identity, social status, privacy and face-keeping in digital society. *Social Science Information,* 47(3), pp. 299-330.

Latour, B. 2005. *Reassembling the social: an introduction to actor-network-theory*. Oxford & New York: Oxford University Press.

Lustig, B.A. 1992. The Method of 'Principlism': A Critique of the Critique. *Journal of Medicine and Philosophy,* 17(5), pp. 487-510.

Mill, J.S. 1879. *Utilitarianism*. London: Longmans, Green, and Co.

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *Ethical Principles and Guidelines for the Protection of Human Subjects of Research* [Online]. Available from: http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html [Accessed 05-04-2012].

Nozick, R. 1974. *Anarchy, State, and Utopia*. New York: Basic Books.

Nussbaum, M.C. 2003. Capabilities as fundamental entitlements: Sen and Social Justice. *Feminist Economics*, 9(2-3), pp. 33-59.

Richardson, H.S. 1990. Specifying Norms as a Way to Resolve Concrete Ethical Problems. *Philosophy and Public Affairs* 19(4), pp. 279-310.

Ross, W.D. 2002. *The Right and the Good*. New York: Oxford University Press.

Sidgwick, H. 1877. *The Methods of Ethics*, London: Macmillan.

Simpson, D.L. 2012. William David Ross (1877-1971) [Online]. *IN:* Frieser, J. & Dowden, B. *Internet Encyclopedia of Philosophy*. 2013. Available from: http://www.iep.utm.edu/ross-wd/ [Accessed 21-03-2013].

Singer, P. 1972. Famine, Affluence, and Morality. *Philosophy & Public Affairs*. 1(3), pp. 229-243.

Sinnott-Armstrong, W. 2011. Consequentialism [Online]. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Winter 2012 Ed. Available from: http://plato.stanford.edu/archives/win2012/entries/consequentialism / [Accessed 20-03-2013].

Smyth, B. 2009. The Sensor Web: Bringing Information to Life [Online]. *ERCIM News*, 76, p. 3. Available from: http://www.clarity-centre.org/files/ECRIM%20News%20Special%20Edition-%20The%20Sensor%20Web.pdf [Accessed 2 June 2011].

Tavani, H.T. & Moor, J.H. 2001. Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society,* 31(1), pp. 6-11.

United Nations. 2013. *Universal Declaration of Human Rights* [Online]. Available from: http://www.un.org/en/documents/udhr/index.shtml [Accessed 14-04-2013].

Winner, L. 1986. The whale and the reactor: a search for limits in an age of high technology. Chicago: University of Chicago Press, 19-39.

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E. & Punie, Y. 2008. *Safeguards in a World of Ambient Intelligence*. Springer.

Prolegomena

2 The technology

Introduction

In this section the definition and characteristics of lifelogging technology are examined.[8] Firstly, as a general consensus on the definition of lifelogs is currently lacking, a working definition is provided. Secondly, the terms 'lifelog device', 'lifelog application', and 'data sources' are elaborated upon. Thirdly, the current state of lifelog technology is discussed. This part contains a brief history of the technology, and an exploration of the goals for which lifelogs can be used, the types of users, and sources of data. Fourthly, uncertainties related to the future development of lifelog technology are examined. Fifthly, the future contingencies and the broad applicability of lifelog technology require a delimitation of research; this research will be further delimited through the use of a scenario.

2.1   Definition of a lifelog

Lifelogs, and the activity of lifelogging, is a new and evolving field consequently a generally accepted definition of lifelogging has yet to be crystallised. This is quite common for a new field of technology. For example, similar examples of technologies whose definitions are still debated are *ambient intelligence* and *synthetic biology*. The lack of a distinct definition is not, however, necessarily permanent. Nanotechnology is an example of a technology that was heavily debated but now has an established definition.[9]

The following working definition of lifelogs will be used in this dissertation: a lifelog is a form of pervasive computing consisting of a unified, digital record about an individual's quotidian activities using data captured multimodally, which are stored and processed by the technology into meaningful and retrievable information to form a personal digital archive of multimedia data.[10]

---

[8] Large parts of this chapter can be found in Jacquemard et al. 2014.

[9] The Oxford dictionary defines it is "[t]he branch of technology that deals with dimensions and tolerances of less than 100 nanometres, especially the manipulation of individual atoms and molecules" (Oxford Dictionary 2014).

[10] This definition is a reworking of the definition of Dodge & Kitchin 2007: "A life-log is conceived as a form of pervasive computing consisting of a unified, digital record of the totality of an individual's experiences, captured multimodally through digital sensors and stored permanently as a personal multi-media archive" (Dodge & Kitchin 2007, 2). Especially the use of "totality of an individual's experiences" which is unclear as well as the focus on digital sensors which is too limited, render this previous definition unsuitable.

This definition has been established as other definitions either seem to miss important characteristics or contain ambiguities. Below is a short explanation of this working definition and the elements it is composed of:

1) The technology is considered a form of pervasive computing. Pervasive computing (which is similar to ubiquitous computing) is the integration of computing to provide connectivity and services at all times and places (Elsevier 2014). Regarding lifelog technology, pervasiveness is in the ability to capture information anywhere at any time and about potentially anything.

2) The data contained within the lifelog are integrated and stored in one place, perhaps on the cloud. The cloud is a service delivered over a network most typically the Internet.

3) Lifelogs generate information about the quotidian activities of the lifelogger. The data can reveal information about the lifelogger directly, or the environment in which she is located as information about the environment can reveal information about her. Some lifelog devices even predominantly capture data about the environment. This is most evident when considering outward facing devices, such as wearable, automatic lifelogging cameras, which take photos of the environment in which one is situated rather than of the physical appearance of the lifelogger.

4) The data gathered come from different devices and in different formats.

5) A lifelog is more than simply the storage of information and also consists of the organisation of the data. In order to make information retrievable about the lifelogger, providing meaning and significance to data and identify things such as events, states, and relationships, is an intrinsic part of the lifelog (DARPA/IPTO 2003). If one was to compare a lifelog with a real-life unsorted collection of photos, say 20,000 photos, which is approximately the amount of photos which could be gathered by a Vicon Revue lifelog device in a week, then it is evident that these photos need to be organised to make the lifelog practical.

6) The result is a personal multimedia archive. The term 'personal' is meant to signify that the lifelog contains the quotidian activities of one particular person rather than anyone else (even though by capturing the quotidian activities of one person, one will often capture information about others as one does not live in solitude). The term 'personal' should not be

interpreted as 'private', 'confidential', 'intimate' or 'secret' even though much personal information within the lifelog might be private, confidential, intimate or secret. Indeed, the term 'personal information' used throughout this work denotes information that affects a person rather than information that is confidential or secret.

2.2 Lifelog devices and applications

Lifelog technology can consists of a wide range of different devices. A lifelog device is either developed for the purpose of lifelogging or it is a device that was originally developed for other purposes, but its functioning has been altered to suit the purposes of lifelogging. The SenseCam is an example of a device, which has been developed for the purposes of lifelogging. Devices that are currently not made for the purpose of lifelogging could be transformed into a lifelogging device by installing an application that alters their functioning, an example of this is the smartphone. Lifelog devices capture, store, process, or allow the lifelogger to query lifelog data. A lifelog application is a piece of software that is designed or implemented to perform a task for the lifelog.

Sometimes the term data source is mentioned in this study. A data source is interpreted as data obtained from a digital portal, application or device that can be added to the lifelog and that reveals information about the lifelogger. Data sources do not have to originate from a lifelog device or application. An eStatement (digital replica of one bank or credit card statement) or digital point-and-shoot cameras can be useful sources of data for lifelogging, but one's online bank-account or digital point-and-shoot camera do not become lifelog devices as their functioning is not changed for the purposes of lifelogging.

2.3 Current state of lifelogs

In the next section, in addition to the history of lifelogs, the various purposes, users, and sources of data are discussed.

2.3.1 Brief history and current state of lifelogs

Lifelogging has been an intriguing idea for some time. The idea surfaced in non-fiction literature before the technology was considered even remotely feasible. In 1945, Vannevar Bush, an American engineer, discussed a device called the 'Memex', which would be a mechanised personal memory supplement (Bush 1945). More recently, Don Norman speculated about a Personal Life Recorder, 'The Teddy' (Norman 1992). The Teddy would be a device that serves as "a personal assistant, small and unobtrusive, that could remember

the details of life for us, so that we could always have them available on demand" (Norman 1992, 72). Another visionary was David Gelernter who described software models that capture a "chunk of reality" (Gelernter 1992, 3) and make it accessible to people on computing devices.

Current technology has long surpassed the idea of the Memex. Gordon Bell and Steve Mann are well-known for gathering personal information to create individual databases of their lives. Mann started wearing a camera in the 1980s, as a precursor to what he calls *lifeglogs*, which can be conceived as a different term for a lifelog (Mann 2004). From 2001 to 2007, Bell, who coined the term 'lifelog' around 2001, digitised all sorts of information about himself, such as the books he read, music he listened to, memos he wrote and he collected photographs using a wearable camera, all for the Microsoft project MyLifeBits (Bell & Gemmell 2009, 29). This can be considered the first explicit lifelogging project. There are also several running projects, most notably that of Cathal Gurrin who has been lifelogging since 2006.[11] Another recent project is that of William McDonough designing "the first living archive" (Fleming 2013).

The US Defense Advanced Research Projects Agency (DARPA) has a track record of developing lifelog-like programmes that capture personal information. Both 'LifeLog', a "system that captures, stores, and makes accessible the flow of one person's experience in and interactions with the world" (DARPA/IPTO 2003), and 'Total Information Awareness' (TIA), a data mining programme used to combat terrorism, were programmes aimed to collect as much information as possible about a person. Both projects had to be withdrawn within two years as a result of controversy, because they were deemed too intrusive to privacy and an infringement of civil freedom (DARPA/IPTO 2003; DARPA 2003).[12]

There is also commercial interest in lifelog technology. Microsoft has developed a camera especially designed for lifelogging, namely the SenseCam, which also featured prominently in the MyLifeBits project (Microsoft 2011).[13] Today, a new generation of

---

[11] More information about his research can be found at http://www.computing.dcu.ie/people/dr-cathal-gurrin [Accessed 30-06-2014].

[12] However, shortly afterwards, similar programmes were established by DARPA such as 'ASSIST' (Advanced Soldier Sensor Information System and Technology) in 2004, which is a project to equip soldiers in a combat zone with sensors in order to augment their memory with digital reports (Schlenoff, Weiss & Potts Steves 2011; Shachtman 2004).

[13] The SenseCam has been rebranded the Vicon Revue. The Vicon Revue surpasses the ability of conventional cameras as it combines various sensors, sensing the environment and the wearer, so that it can react to its

cameras has been developed especially for the purposes of lifelogging, and are or will soon be commercially available, such as the Parashoot, Narrative Clip, MeCam, Autographer, and Looxcie 3. Likewise, Sony has recently announced its own lifelog camera. These are wearable cameras that take photos automatically and that can be worn by the lifelogger. The Narrative Clip, for example, is barely larger than a sizeable postage stamp.

There are also various applications that transform existing devices, most notably the smartphone, into lifelog devices, including Saga, LifeBox, Chronos, and Sony's LifeLog app. These applications support the idea that the smartphone could become a pivotal lifelogging device. The smartphone has several characteristics that make it suitable for becoming a lifelogging device. First, it is firmly embedded into everyday life. Smartphone are often carried around almost everywhere allowing the owner to lifelog most times of the day without having the additional burden of carrying or purchasing a device solely for lifelogging. Also, the smartphone is both equipped with sensors as well as connected to the Internet, allowing the user to capture information about physical conditions as well as information about her Internet behaviour and can send this information to the cloud. Moreover, turning a smartphone into a lifelogging device can be as easy as installing an application.

More devices are now being developed that seem similar to lifelogging devices and can be used for lifelogging. One trend is the rise of the Quantified-Self movement, consisting of devices and applications that quantify aspects of human life. This movement seems to have a similar vision of capturing aspects of an individual's life and making them retrievable but with a narrower focus on numbers. There are numerous wearable devices and applications that fit the Quantified-Self moniker, such as Fitbit, Jawbone UP, Nike's Fuelband, Sony's Smartband, Misfit Shine, *et cetera*. Another development is the creation of ambient intelligent technologies in which devices will increasingly be interconnected and equipped with sensor devices (see *4.2.2.3 Reduced expectation of privacy*). Finally, there are other movements, such as the Internet of Things (Evans 2011: Guillemin & Friess 2009) or the aforementioned Sensor Web (*Introduction*) that motivate the creation of new devices and applications that can capture and distribute personal information.

---

environment by taking more photos when changes are measured. Moreover, interfaces have been designed in order to query and present this information. Therefore, the Vicon Revue in combination with intelligent software can be considered one of the first primitive lifelogs.

Nonetheless, lifelog technology is still at an early stage of development. There is still much space for improvement regarding critical functionalities, such as the augmentation of data with significance and meaning and the related ability to search and find information about elements of one's life. Another area of improvement is the integration of different data sources. There are many potential data sources that can be made compatible with lifelog technology that are at the present not used for lifelogging or are not available to private individuals .

2.3.2 Purposes

The ability to retrieve personal information about the lifelogger's life can serve different goals.

In the most general sense, lifelogs contain information about the behaviour of lifeloggers. Dodge & Kitchin (2007) call the functioning of a lifelog "autobiographical" (Dodge & Kitchin 2007, 7), but this is confusing as it is the lifelog, and not the user that processes data. Rather, a lifelog provides a 'history' or 'biography' of the parts of a person's life that are lifelogged. In this sense, the lifelog is commissioned rather than written by the individual.

Another common metaphor is that of a lifelog as a "portable, infallible, artificial memory" (Bell & Gemmell 2007) but also this metaphor is flawed. The information a lifelog contains can surpass the information one obtains through experience let alone what one can remember. For instance, identification software can recognise people in photos whom one did not notice at the time, GPS and WiFi can track distances more accurately than a person's guess, and a heart rate monitor can measure heart beats. In addition, lifelogs are unable to store particular types of information: although they may capture times, places, names they are unable to store other information that one would remember, such as subjective experience and particular human emotions such as empathy. Finally, memories are dissimilar to data as they are subjective revisions of one's past. In contrast to a photo, which is taken once at a certain point in time, a memory is constructed whenever it is prompted. This process differs at given times and hence one's memory of the past actually changes. These shortcomings are discussed in *3.2.1.3 Shortcomings of the technology*.

The particular uses of a lifelog and motivations for keeping a lifelog are many-fold as the following examples demonstrate:

- Lifelogs can be used to benefit health or improve medical practice. Some authors considered lifelogs or specific lifelog devices to have the potential to serve as a therapeutic tool (Allen 2008; Bell & Gemmell 2009; O'Hara, Tuffield & Shadbolt 2009). The SenseCam, for example, can serve as a mnemonic device to support patients at an early stage of dementia (Piasek, Irving & Smeaton 2011).

- The use can be corporate: This can have productivity goals. By increasing knowledge about the behaviour of employees and feeding back this knowledge, employees may improve their performance at some task or they may even improve because they know that they are being monitored (Rawassizadeh 2011).

- Governmental institutions could profit from lifelogs, either because lifelogs provide them with more information about citizens, which was the case with the DARPA LifeLog project (DARPA/IPTO), or they can equip soldiers with lifelog devices, as is the case with the soldier body suits which are aimed to provide digital memories from the battlefield (Schlenoff, Weiss & Steves 2011, Shachtman 2004).

- Private individuals could also choose to purchase lifelog technology for many different personal reasons. Chen and Jones (2012) have examined the use people would obtain from lifelogs. According to them, the general public wants to use lifelogs to: "re-live the remote or recent past"; "memory backup"; "telling and passing life stories"; "re-use"; "evidences"; "collection and archiving"; and "learning about unknown early age" (Chen & Jones 2012). The Narrative Clip, for example, is marketed for such applications.

2.3.3 Users

As there are many potential goals, lifelogs can be designed for a variety of potential users. It is possible to distinguish at least four different types of users:

- <u>Private individuals</u>: Individuals can create a lifelog about themselves for private purposes. These individuals can use lifelog technology to retrieve information from their past. This group is the one discussed within this dissertation.

- <u>Corporations</u>: Corporations could use lifelogs by means of equipping employees with lifelog devices. Currently, Stanford University is developing a *life archive*, which seems like a lifelog, about William McDonough's working life as a sustainable architect

(Fleming 2013). Also, lifelog can be held by corporations to monitor the behaviour of staff with the aim of improving their efficiency or safety.

- Public institutions: Public institutions can also use lifelogs by providing patients with lifelog equipment. Medical institutions may use lifelogs as some treatments and therapies can improve or depend on the monitoring of patients. Work has already been conducted on lifelogs for dementia patients (Piasek, Irving & Smeaton 2011). Also, Universities could use lifelogs as an instrument to obtain data for all kinds of research or advance their technological abilities.

- Governmental organisations: Despite DARPA's LifeLog and ASSIST (DARPA/IPTO 2003; DARPA 2010) projects, also governmental organisations are mostly neglected as a potential user. Lifelog devices could be used by government agencies, for example, to monitor soldiers in battle.

2.3.4 Sources of data

There is a broad range of devices which can be (made) suitable for lifelogs or that can offer useful data for lifelogs. Whilst the ethical relevance may not be immediately clear, this distinction is ethically relevant because the devices will trigger different ethical concerns as both the manner and the information obtained is relevant. Unfortunately an overview of all devices cannot be given as future development leaves open the exact devices which will be used. Nonetheless, the general characteristics of these devices can be distinguished:

- Wearable devices: Wearable devices are devices that function while carried on the body. Narrative Clip, ZEO – a device that measures sleep quality – and the Vicon Revue are wearable.

  - Inward facing devices: These wearable devices measure and capture physical conditions of the individual such as heart rate, glucose levels, and body temperature.

    - Implantable sensor devices: A particular subset of these devices is invasive, i.e. they are in the body. This has ethical relevance especially if the devices are imposed on the lifelogger by third parties, such as governments or corporations, as this could entail violations of bodily

integrity. An example of such a device would be a subcutaneous sensor device which measures glucose using blood samples.

- Outward facing devices: These devices capture physical conditions about the environment instead of the individual. Examples are the Vicon Revue and Narrative Clip, capturing the environment in which the individual is situated rather than the individual.

- Online activities: Not all data are captured by sensors that measure physical conditions. Some of the data are about digital activities, such as visited websites and emails, and can be sourced from any wearable device which allows one to participate in the digital realm.

- Environmentally embedded devices: These devices are embedded in the environment in which the person is situated rather than worn by the individual. Examples of such devices are energy usage meters, smart televisions, or magnetic stripe card holders when entering a room or building.

- Online activities: Same as above. Examples of devices are desktop computers or smart televisions.

- Third party information: Some data are obtained from third parties. Different third parties could provide data that reveal personal information about the individual, such as financial or health institutions.

2.4 Future development

As lifelog technology is at an early stage of development. There are uncertainties regarding its future development that complicate an inquiry. The shape, use and regulation of this technology are dependent on a myriad of influences from the social, political, ethical, scientific and technological sphere (McGregor & Wetmore 2009). A few important future uncertainties are mentioned below:

- The number of people that will use lifelog technology is currently unknown. The reach of lifelog technology is ethically relevant, because some ethical concerns are partly determined by consumer numbers. The effect of lifelogs on privacy is of a lesser concern when just a few people use lifelogs. Also, the authorities might have less interest in institutionalising access to lifelogs when only a small number of people lifelog.

- The influence of lifelogs is partly dependent on social norms that set boundaries to the recording and sharing of information. Social norms are important when determining whether to record an event. Taking photographs in some cases is considered inappropriate, and therefore someone might refrain from recording. In addition, social norms may determine the purposes for which lifelogs are used. Those norms might change with the introduction of new technology (Bijker 1995; Latour 1994; Latour 2005a; Latour 2005b).

- Legal limitations on the access, spread, deployment, and manipulation of lifelog technology will influence the effect of lifelog technology on users and society at large and the adequateness of checks and balances in place to curb the power of corporations or governments can be lacking. However, those laws are subject to change.

- The devices and data sources which are (made) suitable for lifelogging and the information lifelogs can infer from data is uncertain. An increasing amount of devices are equipped with digital sensing devices and have network functionality and can, therefore, be made suitable as a data source for lifelogging.[14] In addition, users, individuals, authorities, and companies are more active online, leaving more digital traces.

- The platform on which lifelog information is accessible is unknown: lifelog information could be accessed on personal computers, mobile computing devices such as tablet, smartphones or laptops or wearable devices such as Google Glass. In addition, measures to secure these platforms and the success of the security are uncertain.

- The retrieval of information is another variable. Newly developed algorithms make it possible to extract novel information and/or provide more detailed information using existing data. In addition, the choice to implement certain search features and other functionalities within the design of the technology is partly dependent on the choices of developers. Furthermore, lifelog technology may provide information automatically through prompts or the lifelog could only provide information when queried by the user.

---

[14] One of the most pivotal devices with regard to lifelog technology will be the smartphone, since it could harvest tremendous amounts of information. It is able to gather digital and non-digital information being equipped with multiple sensors, used for online activities and as a communication device. Moreover, the smartphone is easily connected to other devices or the Internet which facilitates its functioning as a hub to spread and receive information. A simple tweak could make the smartphone take photos automatically.

The uncertainty surrounding the further development of lifelogs should not be considered idiosyncratic to lifelogs. It is inherent of an emerging technology that its features, uses, and popularity are unknown (Collingridge 1980, Liebert & Schmidt 2010). This complicates the ethical inquiry. However, the need for an ethical assessment persists.

Collingridge (1980) formulated a dilemma when discussing ethical concerns about technology at an early stage of development. He stated that "when change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time consuming" (Collingridge 1980). Consequently, potential issues either need to be addressed at an early stage of development when information is limited, or the technology becomes embedded and the ability to address challenges has decreased.

It might be impossible to predict the future without significant uncertainty, but it is possible to discuss a state of affairs one desires to accomplish or avoid. Indeed, the value of discussing ethical challenges at an early stage of development is to meet them and to avoid a particular state of affairs that is predicted to potentially arise.

2.5   Scenario

A plausible future scenario is used to delimit the research and illustrate some ethical concerns of interest. Since the technology is still at this stage of development, a scenario is generally an acceptable way to consider potential normative ethical issues.

In this scenario, certain features of the technology are presupposed, as if they have been already developed. This scenario is not intended as an accurate prediction of the future. Instead, a scenario such as this one provides an idea of a future, which can be used to discuss the potential merits and demerits of the technology (Wright et al. 2008). Even though the scenario is fictional, the feasibility of the scenario will be substantiated by referring to current research. The use of the proposed scenario is instrumental, i.e. the scenario will not be an end in itself.

In this scenario, an average day of a plain Jane using a lifelog is depicted. The numbers within the scenario correspond with potential issues: (1) privacy, (2) autonomy, and (3) beneficence:

Lifebook

After a long day at the office, Paula decides to take a look at her lifelog by opening the lifelog application on her tablet computer. The lifelog can be accessed through web browsers as well – which allows her to access her lifelog at any place and time with an Internet connection. (1) Her lifelog is conveniently stored in a cloud somewhere in the US where the company, Lifebook, which offers the lifelog service, resides. (1) She is unaware that her information is not kept in Ireland, although this information was made available to her in the terms and conditions (Celestine 2012). (2)

Initially she did not want to keep a lifelog, but friends of hers were early adopters using the lifelog to improve their diet, keep track of their sleep, exercise, cultural activities, travels and TV-habits, and they shared this information on their Social Networking profiles and on Internet forums encouraging each other to improve their lives. (1) (2) (3) She wanted to be a part of these groups. (2) Another reason for her to use lifelogs was that her friends had transcripts, audio, video, and photos of most of their conversations with her which made her feel vulnerable as she did not have the information herself. (2) She chose the most popular service which has virtually all of the lifelog market consisting of 400,000 people in Ireland alone and is still growing (Mulley Communications 2013). (1)

The maintenance of the lifelog costs her little time and effort. (1) Partly because most technology is hidden within devices she would use anyway. Her glasses contain a camera and a microphone (Google 2013a). They can be switched off by using a simple voice command, and they recognise situations unsuitable for the lifelog such as bathroom visits (Google 2013a). This can be problematic, as some bathrooms are not recognised as such by the software - especially in hotels and venues, such as nightclubs or expensive restaurants, in which the interior decoration is slightly different than generally at home or in offices. This has caused some embarrassing moments when reviewing her lifelog information. (1) Her telephone captures her whereabouts and her physical activities (GPS Tracks 2013; Runkeeper.com 2013). The vest she wears under her dress senses physical data, namely her heart rate, body temperature, blood pressure and even her breathing, as does her pyjama top (López, Custodio & Moreno 2010; Fang 2011). The wristband she wears tracks her exercise levels (Jawbone 2014). She has a baseball hat measuring electric signals in the brain, but she does not really like the look of it so she never uses it. She only uses a headband to measure electrical signals of the brain during her sleep (ZEO 2013).These sensors cannot be switched

off once worn although the data can later be deleted from the lifelog. Furthermore, her desktop computer, tablet, smartphone, and her television log her email, visited websites, chats, telephone calls, watched television programmes and text messages. (1) Except for video and audio, she mostly keeps them lifelogging whenever she wears or uses them, as, according to her, they do not reveal much about her. (1)(2)

Once the devices are linked up, the lifelog gathers the data through wireless networking technologies. Paula can choose which information she makes visible to herself. (2) She is mainly interested in her health and the information that is directly visible are her diet, her physical activities, her sleep, and her stress levels measured by her blood pressure, heart rate, breathing and her brain signals (Affectiva 2013; Athos 2014; ZEO 2013: Barua, Kay & Paris 2013). (3) Some information is hidden from her, but is still created. (2) She hides some information, such as the activities or persons which caused her most stress, as she has had embarrassing results. (2) The information hidden from the lifelog by the user is kept by the company although not available to users. The company keeps information because it might be useful for advertising purposes. It is unclear what information the company exactly gathers from lifelogs. (1)

Lifebook does not sell data about individual people to other parties, but guarantees its confidentiality within legal limitations of the law (Facebook 2013; Instagram 2013). (1) However, they do sell de-identified, personal information in bulk. (1) They get requests to hand over information quite frequently as they are the most popular lifelog service (Google 2013b; Twitter 2013). Paula is unaware of this, although the company publicises the frequency of which data are requested as an aggregate. Lifebook employees have no access to the cloud. (1) Individual users are not notified when their information is being subpoenaed. (2) The company also offers advertisers the opportunity to target specific groups. (2) The company allows advertisers to draw up a specific target group and deliver this information to that group. Sometimes it highlights particular information as it might be beneficial for the advertisers with the occasional advertisement. The company could choose to present the lifelogger with a photo with the logo of the brand when someone is looking for a past event rather than another photo. For example, when Paula is retrieving information about a night out, the first result is often one with her laughing and the advertisement of a particular brand of beer – even when she did not drink it – in the background. The lifelog company does not inform the lifelogger about specific interventions so Paula would not know that this photo is shown for purposes of advertisement, but the terms and conditions allow

them. (2) This is how the lifelog company makes its money as they do not charge subscription fees.

Today, Paula wants to look up a specific person, a new colleague. She is allowed to lifelog at work, as long as she stops certain lifelog data as video and audio recordings during important meetings. (1) It does not take long for the lifelog application to find him because the introduction of him as the new manager has been marked as a significant event that day (Shachtman & Beckhusen 2013). She is curious if she has met him before and when she queries the lifelog, it shows photos of him at a party three years ago. She looks at the photos of him at the party and realises to her dismay that she had gotten horribly drunk that night which she usually does not (University of Pittsburgh 2013). (1) In fact, this is the only time she consumed this many alcoholic beverages in the last three years of her keeping the lifelog. (3) After the initial shock, she soon discovers that he might have been worse off as he looked particularly bad in the photos. Also he did not seem to be wearing a lifelog camera. (1) So fortunately, it seems unlikely that he would have photos of her unless he was using a very small or camouflaged device. The second thing she wants to look up is some information she wants to share. Her insurance gives her minor discounts when she can provide some information about her exercising, which she does only because it takes so little effort (Aviva 2013). (2) (3) The lifelog indicates that she eats healthily, although her diet lacks calcium and the mineral iron together with an advertisement for an online health shop which offers supplements. (2) (3) The third thing she wants to look up is the time spent with her children. She retrieves the times she was with her children by searching for hours spent, which reassures her that she has been around them enough lately. (2) She shares this information on her Social Networking Site, as she is proud of this achievement. (1)

Bibliography

Affectiva. 2013. *Q Sensor 2.0* [Online]. Available from: http://www.affectiva.com/q-sensor/ [Accessed 20-03-2013].

Allen, A.L. 2008. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74.

Athos. 2014. *Athos: Wearable Technology for Fitness* [Online]. Available from: http://www.liveathos.com/ [Accessed 09-09-2014].

Aviva. 2013. Insurance discount for safe drivers with Aviva Drive [Online]. Available from: http://www.aviva.co.uk/drive/ [Accessed 11-04-2013].

Barua, D., Kay, J. & Paris, C. 2013. Viewing and Controlling Personal Sensor Data: What Do Users Want? *IN: Lecture Notes in Computer Science Volume 7822,* pp 15-26.

Bell, G. & Gemmell, J. 2007. A Digital Life. *Scientific American*. Available from: http://www.scienceandsociety.org/web/Library_files/A.Digital.Life.pdf. [Accessed 28-05-2012].

Bell, G & Gemmell, J. 2009. *Total Recall: How The E-Memory Revolution Will Change Anything*. New York: Dutton.

Bijker, W.E. 1995. *Of bicycles, bakelites, and bulbs : toward a theory of sociotechnical change.* Cambridge: MIT Press.

Bush, V. 1945. As we may think. *The Atlantic Monthly,* 176(1), pp. 101-108.

Celestine, A. 2012. Cloud computing: How tech giants like Google, Facebook, Amazon store the world's data [Online]. *The Economic Times*. Available from: http://articles.economictimes.indiatimes.com/2012-05-27/news/31860969_1_instagram-largest-online-retailer-users [Accessed 20-03-2013].

Chen, Y. & Jones, G.J.F. 2012. What do people want from their lifelogs? *IN: 6th Irish Human Computer Interaction Conference*.

Collingridge, D. 1980. *The social control of technology*. New York: St. Martin.

DARPA. 2003. *'Terrorism Information Awareness' (TIA) Program formerly known as 'Total Information Awareness'* [Online]. Available from: http://www.iwar.org.uk/news-archive/tia/total-information-awareness.htm [Accessed 30-01-2012].

DARPA/IPTO. 2003. BAA # 03-30 *LifeLog Proposer Information Pamphlet* [Online]. Available from: http://realnews247.com/lifelog.htm [Accessed 30-01-2012].

DARPA. 2010. *Advanced Soldier Sensor Information Systems and Technology (ASSIST)* [Online]. Available from: http://www.darpa.mil/Our_Work/I2O/Programs/Advanced_Soldier_Sensor_Information_Systems_and_Technology_(ASSIST).aspx [Accessed 30-01-2012].

Dodge, M. & Kitchin, R., 2007. Outlines of a world coming into existence': pervasive computing and the ethics of forgetting. *Environment and Planning B Planning and Design*, 34(3), pp.431-445.

Elsevier. 2014. *Pervasive and Mobile Computing* [Online]. Available from: http://www.journals.elsevier.com/pervasive-and-mobile-computing [Accessed 04-02-2014].

Evans, D. 2011. *How the Internet of Things Will Change Everything—Including Ourselves* [Online]. Available from: http://blogs.cisco.com/news/how-the-internet-of-things-will-change-everything%E2%80%94including-ourselves/ [Accessed 31 May 2011].

Facebook. 2013. *Legal terms* [Online]. Available from: https://www.facebook.com/legal/terms [Accessed 20-03-2013].

Fang, J. 2011. Smart shirt monitors your breathing while you sleep [Online]. Available from: http://www.smartplanet.com/blog/rethinking-healthcare/smart-shirt-monitors-your-breathing-while-you-sleep/4699 [Accessed 20-03-2013].

Fleming, N. 2013. I'm recording everything for the first living archive [Online]. *NewScientist.com*. Available from: http://www.newscientist.com/article/mg21829110.300-im-recording-everything-for-the-first-living-archive.html [Accessed 10-04-2013].

Gelernter, D. 1992. *Mirror Worlds: Or The Day Software Puts the Universe into a Shoebox… How it will happen and what it will mean.* Oxford: Oxford University Press.

Google. 2013a. *Glass* [Online]. Available from: http://www.google.com/glass/start/ [Accessed 20-03-2013].

Google 2013b. *Transparency Report* [Online]. Available from: http://www.google.com/transparencyreport/userdatarequests/ [Accessed 20-03-2013].

GPS Tracks. 2013. *GPS Tracks* [Online]. Available from: http://gpstracksapp.com/ [Accessed 20-03-2013].

Guillemin, P. & Friess, P. 2009. *Internet of Things Strategic Research Roadmap* [Online]. Available from: http://sintef.biz/upload/IKT/9022/CERP-IoT%20SRA_IoT_v11_pdf.pdf [Accessed 15 April 2011].

Instagram. 2013. *Terms of Use* [Online]. Available from: http://instagram.com/legal/terms/ [Accessed 20-03-2013].

Jacquemard, T., Novitzky, R., O'Brolcháin, F., Smeaton, A.F. & Gordijn, B. 2014. Challenges and opportunities of lifelog technologies: a literature review and critical analysis. *Science and Engineering Ethics*, 20(2), pp. 379-409.

Jawbone. 2014. *UP* [Online]. Available from: http://jawbone.com/store/buy/up [Accessed 17-06-2014].

Kelly, P., Kumar, A., Doherty, A.R., Lee, H., Smeaton, A.F., Gurrin, C. & O'Connor, N.E. 2010. The colour of life: interacting with SenseCam images on large multi-touch display walls [Online]. *SenseCam 2010 - second annual SenseCam symposium* Available from: http://doras.dcu.ie/15707/ [Accessed 23 November 2012].

Latour, B. 1994. On Technical Mediation - Philosophy, Sociology , Genealogy. *Common Knowledge* 3(2): 29-64.

Latour, B. 2005a. *Reassembling the social: an introduction to actor-network-theory.* Oxford & New York: Oxford University Press.

Latour, B. 2005b. From Realpolitik to Dingpolitik. Or how to make things public. In: Latour, B. & Weibel,P. (eds.) *Making things public. Atmospheres of democracy*. Cambridge: MIT Press.

Liebert, W. & Schmidt, J.C. 2010. Collingridge's dilemma and technoscience: An attempt to provide a clarification from the perspective of the philosophy of science. *Poiesis & Praxis*, 7(1-2).

López, G., Custodio, V. & Moreno, J.I. 2010. LOBIN: E-Textile and Wireless-Sensor-Network-Based Platform for Healthcare Monitoring in Future Hospital Environments. *IEEE Transactions on Information Technology in Biomedicine*, 14(6), pp. 1446-1458.

Mann, S. 2004. "Sousveillance" Inverse Surveillance in Multimedia Imaging. *MULTIMEDIA '04 Proceedings of the 12th annual ACM international conference on Multimedia,* pp. 620-627.

McGregor, J. & Wetmore, J. 2009. Researching and Teaching the Ethics and Social Implications of Emerging Technologies in the Laboratory. *NanoEthics*, 3(1), pp. 17-30.

Memoto. 2013. *Memoto Automatic Lifelogging Camera* [Online]. Available from: http://memoto.com/ [Accessed 15-01-2013].

Microsoft. 2011. *Microsoft Research SenseCam* [Online]. Available from: http://research.microsoft.com/en-us/um/cambridge/projects/sensecam/ [Accessed 30-01-2012].

Mulley Communications. 2013. *Facebook doubles in size in Ireland in 12 months – 400k in January 09* [Online]. Available from: http://mulley.ie/blog/2009/01/facebook-doubles-in-size-in-ireland-in-12-months-400k-in-january-09/ [Accessed 20-03-2013].

Norman, D. 1992. *Turn Signals are the Facial Expressions of Automobiles*. Cambridge: Perseus Publishing, pp. 72-85.

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

Oxford Dictionaries. 2014. *Nanotechnology.* Available from: http://www.oxforddictionaries.com/definition/english/nanotechnology [Accessed 05-07-2014].

Piasek, P., Irving, K., & Smeaton, A.F. 2011. *SenseCam Intervention Based on Cognitive Stimulation Therapy Framework for Early-Stage Dementia* [Online]. Available from: http://doras.dcu.ie/16838/ [Accessed 22 November 2012].

Rawassizadeh, R. 2011. Towards sharing life-log information with society. *Behaviour & Information Technology*, pp. 1-11.

Runkeeper.com. 2013. *RunKeeper* [Online]. Available from: http://runkeeper.com/home [Accessed 20-03-2013].

Schlenoff, C., Weiss, B. & Potts Steves, M. 2011. A Retrospective Analysis of Lessons Learned in Evaluating Advanced Military Technologies. *ITEA Journal of Test & Evaluation,* 32(4), pp. 471 – 478.

Shachtman, N. 2004. Pentagon Revives Memory Project [Online]. *Wired.com*. Available from: http://www.wired.com/politics/security/news/2004/09/64911 [Accessed 30-01-2012].

Shachtman, N. & Beckhusen, R. 2013. 11 Body Parts Defense Researchers Will Use to Track You [Online] Wired.com. Available from: http://www.wired.com/dangerroom/2013/01/biometrics/?pid=1775&viewall=true [Accessed 25-01-2013].

Twitter. 2013. *Transparency Report* [Online]. Available from: https://transparency.twitter.com/information-requests [Accessed 25-01-2013].

University of Pittsburgh. 2013. Basic Science Projects: Unified Sensor System for Ubiquitous Assessment of Diet and Physical Activity [Online]. Available from: http://www.neurosurgery.pitt.edu/research/projects/basic_science/diet_sensor.html [Accessed 20-03-2013].

Vicon Revue. 2013. *Revue applications*. 2013. Available from: http://viconrevue.com/applications.html [Accessed 30-01-2013].

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E. & Punie, Y. 2008. *Safeguards in a World of Ambient Intelligence*. Springer.

ZEO. 2013. *ZEO* [Online]. Available from: http://www.myzeo.com/sleep/ [Accessed 20-03-2013].

3 Literature Review

Introduction

This chapter maps the main ethical challenges and opportunities associated with the further development of lifelog technologies, as discussed in the scholarly literature as uncovered. At first, the method used to select the relevant sources is explained. Next, the results of the review are presented. In the last part, the results are critically discussed by highlighting several issues previously left undebated.[15]

3.1   Method

The Google Scholar database was used to find relevant sources. The first limitation was selecting English language material only. The search results were judged by reading the abstract. The whole article was skimmed in the case of missing abstracts. The second limitation was that the content had to involve ethical considerations on contemporary lifelog technology as discussed here. This latter criterion ruled out Bush's article about the Memex, which was still a far cry from current technologies. Also, sources discussing a radical different technology from what is understood here to be a lifelog, such as a lifelog as a weblog, were left out of this literature review.[16] The third limitation, partly arising from the previous, was limiting the search to articles from 2001 onwards. The year in which the MyLifeBits project started, creating the idea of lifelog technology in its current form. The fourth limitation entailed that sources had to elaborate on ethics. Therefore, sources mentioning applications to research ethics committees, or acknowledging potential ethical issues without explaining or explicitly materialising them in their research are omitted from this literature review as they do not constitute an advancement of the ethical debate.

The terms "lifelog" and "ethic" were searched, specifying that the words must occur anywhere in the article.[17] It yielded 348 results, 30 of which were used in this review (Allen

---

[15] Large parts of this chapter have been published (Jacquemard et al. 2014).

[16] As for the large amount of sources not included, this has various reasons of which a few examples will be provided: the term 'lifelog' used in the source signifies a radically different technology such as a weblog; in the source a reference has been made to lifelog devices or projects, but these are not the focus of inquiry; sources can mention the existence of ethical issues, only to mention that those do not fall within the scope of their research; applications to Research Ethics Committees as a formal procedure are mentioned but ethical concerns are not discussed; or the terms 'life' and 'log' appear closely together in the texts without mentioning the technology, leading to *false positives*.

[17] The term 'ethic' instead of 'ethics' or 'ethical' to include variations on ethic such as ethical and ethics. The same applies for the term 'moral', which also includes variations such as morality and morals.

2008; Byrne, Kelly & Jones 2010; Clowes 2012; Clowes 2013; Dib 2008; Dib 2012; Dodge & Kitchin 2007; Dodge 2007; Van den Eede 2011; Del Giudice & Gardner 2009; Jayaram 2011; Kang et al. 2011; Kelly et al. 2013; Koops 2011; Lemos 2010; Mann 2004a; Mann 2005a; Moreno 2004; Murata 2011; O'Hara & Hall 2008; O'Hara, Tuffield & Shadbolt 2009; O'Hara 2010a; O'Hara 2010b; O'Hara 2012; Price 2010a; Price 2010b; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Sonvilla-Weiss 2008; Sweeney 2004). Then the term "ethic" was changed to "moral", which yielded one used source (Van Dijck 2012) and "moral" to "normative", which yielded no sources that met the criteria. For the next queries, the same searches were conducted, only replacing "lifelog" with "MyLifeBits" , "MyLifeBits" with "SenseCam" and "SenseCam" with "cyborglog", and combined each of these terms with "ethic", "moral" and "normative" as described in the first search. The last search replaced both "cyborglog", and "normative" with "Steve Mann" and "lifelog". The results are listed in Table 1, which lists the number of results yielded by a search term under 'total', the number of results which did not occur in previous queries under 'new', and the sources which are used in this literature review under 'useful'.[18]

The first queries, "lifelog" and "ethic", "moral" and "normative" are self-explanatory. The second term "MyLifeBits" was chosen because MyLifeBits was an early and pivotal lifelog project. The query "MyLifeBits" and "ethic" provided four used sources (Bannon 2006; Bannon 2011; Curry 2007; Turkle 2011), and the query "MyLifeBits" and "moral," three (Hall, Johansson & de Léon 2013; Katz & Gandel 2008; Lahlou 2008). This third term, "SenseCam," was chosen because the SenseCam is one of the first devices designed especially for lifelogging and worn by prolific researchers such as Gordon Bell and Cathal

---

[18] The literature review may not exhaustively include all sources on the ethical debate on lifelogs. The literature review differs from studies such as the one undertaken by Heersmink et al. 2011 that provide an insight into the relations between key terms in the field of computer and information ethics as mentioned in particular databases using software. Their endeavour provided the academic field with an insight into the frequency in which combinations of terms occur in selected journals. A disadvantage of this approach is that one obtains very little insight into the debate except for the terms used. My aim is to provide a more in-depth insight by providing references to specific sources and by briefly explaining the core of their arguments. This way, researchers can use my literature review to find sources which point them to challenges and opportunities. Unfortunately, this approach is more demanding leaving it unfeasible to incorporate a plenitude of search terms as they were included by Heersmink et al 2011. Therefore terms have been excluded such as 'privacy', 'surveillance', 'autonomy'. In addition, it needs to be stressed that by limiting research to particular databases and journals, one can never be sure to have included all important sources. This applies equally to this literature review as to Heersmink et al. 2011. This concern can be somewhat alleviated through the method of snowballing as influential articles would often be referred to by others. More importantly, the aim of this research is not necessarily to gather all relevant sources. The aim is to set an agenda both for engineers as they may become aware of ethical issues previously unknown to them and for ethicists as they may discover underdeveloped areas within the current debate.

Gurrin. The query "SenseCam" "Ethic" only yielded one result (Weber 2010).The fourth term "cyborglog" has been chosen because of the importance of Steve Mann, considered a pioneer of lifelog technology. The terms 'cyborglog' or 'lifeglog', are the terms he uses for technology similar to lifelogs. The term "cyborglog" "ethic" yielded two usable results (Mann 2005b; Mann, Fung & Lo 2006). The terms "Steve Mann" and "lifelog" have been chosen as the term "cyborglog" seemed less commonly accepted as "lifelog". This yielded four results which were used in this literature review (Mann 2004b; Nack 2007; Sellen & Whittaker 2010; Werkhoven 2005). Before starting this endeavour, the main project, names and technologies were identified. All those queries were conducted on the 8th and 9th of April 2013. Snowballing yielded seven further results (Bailey & Kerr 2007; Bell & Gemmell 2009; Cheng, Golubchik & Kay 2004; Van Dijck 2005; O'Hara et al. 2006; Smith, O'Hara & Lewis 2011; Turkle 2008).

Query	Total	New	Useful
Lifelog ethic	348	-	30
Lifelog moral	96	38	1
Lifelog normative	96	35	-
MyLifeBits ethic	159	84	4
MyLifeBits moral	69	15	3
MyLifeBits normative	20	5	-
SenseCam ethic	194	96	1
SenseCam moral	76	19	-
SenseCam normative	45	15	-
Cyborglog ethic	28	18	2
Cyborglog moral	15	3	-
Cyborglog normative	4	-	-
Steve Mann lifelog	98	55	4

Table 1: Search results

3.2 Results

The searches resulted in 52 relevant sources (23 journal articles, eleven book chapters, eight conference papers, six workshop papers, one book, one column – in a scientific journal –, one talk, and one working paper) after discounting the overlapping entries. Table 2 shows the sources and their year of publication. The debate got started by the aforementioned DARPA project 'Lifelog' (Moreno 2004; Sweeney 2004) and the researchers Mann and Bell (Mann 2004a; Mann 2004b; Cheng, Golubchik & Kay 2004).[19]

Year	Sources
2004	5
2005	5
2006	3
2007	5
2008	6
2009	3
2010	8
2011	10
2012	4
2013	3

Table 2: Year of publication

3.2.1 Challenges

Eight challenges were distinguished from this accumulated literature (see Table 3), which will be elaborated on in decreasing order of frequency of occurrence in the academic debate.

Challenge	Occurrence
Privacy	26
Deleterious influences on perception	18
Shortcomings technology	16
Impeding forgetting	13
Uncertainties	12
Impairing social interaction	7
Psychological and Health risks	5
Issues concerning the protection of research subjects	3

Table 3: Overview of Challenges

---

[19] Cheng, Golubchik & Kay (2004) took part in the CARPE 2004 workshop chaired by Jim Gemmell, who is a partner of Bell on the MyLifeBits project.

3.2.1.1 Infringements on privacy

Lifelogs are said to be detrimental to privacy. However, privacy is often ill-defined or not defined at all, making it puzzling what the scholars meant by the term 'privacy' in different sources. This is arguably the case in the following sources: Byrne, Kelly & Jones 2010; Cheng, Golubchik & Kay 2004; Del Giudice & Gardner 2009; Price 2010a; Price 2010b; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Smith, O'Hara & Lewis 2011; Sweeney 2004; Werkhoven 2005. Most sources suppose an intuitive idea of privacy as the control over personal information. Some have explicated their concept of privacy (Allen 2008; Jayaram 2011; Mann 2005a). Others aimed to redirect a misconception about privacy with regard to lifelogs.[20] One scholar offers an elaborate discussion and provides recommendations for developers (Lahlou 2008).

If privacy is considered to be influenced by control and access of personal information and monitoring, at least, consent should be considered a related challenge. There are consent issues which have been mostly addressed without explicitly mentioning consent.[21] The non-consensual logging of third parties is an obvious challenge (Allen 2008; Bailey & Kerr 2007; Cheng, Golubchik & Kay 2004; Del Giudice & Gardner 2009; O'Hara 2010a; O'Hara 2012; Sonvilla-Weiss 2008). It might become impossible to stay off the grid (Sonvilla-Weiss 2008). Another issue is the freedom to choose to keep a lifelog. There might be considerable societal pressure to keep a lifelog (Allen 2008; O'Hara 2010a; O'Hara 2012). A lifelog could become a prerequisite to show good intentions, since the absence of a lifelog could be interpreted as signifying the intention of hiding malign behaviour. Also, the consequences of sharing information are unclear. Although one might be able to choose the information one wants to share, one has little influence in how self-publicised information is used and interpreted (Bailey & Kerr 2007; Murata 2011). For example, videos can be edited to use only certain parts. Also one has little insight into the retention and functioning of the data.

Another related challenge is surveillance. The relation between citizens and authorities or companies may be affected by lifelogs, as they could be a source of information

---

[20] Kang et al. (2011) explicitly had a privacy account which has control as a central value. Some considered privacy a public good instead of an individual interest (O'Hara et al. 2006; O'Hara, Tuffield & Shadbolt 2009; O'Hara 2010a; O'Hara 2012). Bailey & Kerr (2007) tried to redress the idea of privacy as an individual interest trumped by waivers and consents.

[21] Bailey & Kerr 2007 mention it explicitly as they consider the lack of clarity of the consequences of sharing information.

for states (Allen 2008; Bailey & Kerr 2007; Del Giudice & Gardner 2009; Dodge & Kitchin 2007; Lemos 2010; Moreno 2004; O'Hara, Tuffield & Shadbolt 2009; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Sonvilla-Weiss 2008; Weber 2010). Consequently, citizens are vulnerable to pernicious surveillance by either governmental institutions or corporations (Bailey & Kerr 2007; Del Giudice & Gardner 2009; Dodge & Kitchin 2007; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Sonvilla-Weiss 2008; Weber 2010). Indeed, by using lifelogs citizens can be turned into recreational spies as well as revealing confidential information (Allen 2008; Dodge & Kitchin 2007). Recreational spies, meaning people who investigate without it being their profession, might have little awareness of the legal and moral interests of their target and lack the professional ethics which professional investigators are assumed to possess (Allen 2008, 20).

3.2.1.2 Deleterious influences on perception

Lifelogs have been ascribed a potentially deleterious influence on one's perception of the past, one's memories, and the present, with three specific examples.[22] Firstly, there is a blurring of past and present. The longevity of digitised information renders information about the past as readily available as information of the present. Consequently, the past will be judged with standards of the present and vice versa (Allen 2008; O'Hara 2010a; O'Hara 2010b; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011). A related challenge is the amount of information created: trivial data might marginalise important information (Allen 2008; Katz & Gandel 2008). The source of information changes as well. Lifelogs produce information without a social community (Curry 2007). This will extend a solipsistic view of the world and oneself. Moreover, lifelogs might lead to epistemological uncertainties because data are easily manipulated and therefore not always to be trusted (O'Hara et al. 2006; O'Hara 2010b; Weber 2010).

Second, lifelogs have difficulties capturing subjective experiences and are able to capture only concrete information. This might limit the interest in subjective interpretations. Therefore, in memories, values such as truth might become overstated, narrowing the use of memory (Dib 2008; Van Dijck 2005; Van Dijck 2012; O'Hara 2010a; O'Hara 2012). For instance, memories are also relevant to the composition of identity (Dib 2008). By leaving the archiving of information to devices, one's control over personal information and the way one

---

[22] Sources mentioning challenges within this category are: Allen 2008; Bannon 2011; Curry 2007; Del Giudice & Gardner 2009; Nack 2005; O'Hara et al. 2006; O'Hara 2010a; O'Hara 2010b; O'Hara 2012; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Sonvilla-Weiss 2008; Turkle 2011; Weber 2010

perceives oneself and others are affected. An additional challenge is one's assessment of past behaviour. Lifelogs provide retrospection of decisions made in the past. However, the right decision might be more obvious in hindsight with lifelog information than it was at the time, leading to callous judgements about the past (Bannon 2011; Del Giudice & Gardner 2009; O'Hara 2010a; O'Hara 2012).

Third, lifelogs could influence one's perception of the present. A loss of interest in information that cannot be archived in a lifelog could occur (Turkle 2008; Turkle 2011). Also, lifelogs might have a similar effect on perception as the photo camera, which has made people look at reality as potential photo opportunities (Van Dijck 2005). Even one's existence could be affected; the ability to obtain information from anywhere at any time and the source of information, could change people's understanding of being present (Weber 2010). This challenge is based on the idea that one's perception of the world is based on information rather than objective facts (Weber 2010). Lifelog technology would change information and, therefore, possibly one's perception.

3.2.1.3   Shortcomings of the technology

The functioning of lifelogging technologies has been questioned. Some of these challenges are practical, such as the inconvenience of wearing devices; unintentional lifelogging (i.e. lifelogging without being aware that one is lifelogging); the distress caused by the loss of data; the practical limitations of the devices; the inconveniences of knowing that they are being recorded imposed on others (Bell & Gemmell 2009; Byrne, Kelly & Jones 2010; Mann 2004a; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011). O'Hara (2010a) argued against these challenges, stating that if the technology does not function according to standards, people will refrain from using it. Thus, these challenges will primarily be a practical issue for developers.

However, there are other, more intricate challenges. One of them is that lifelogs might be unable to capture relevant information. The physical world is too complex for all aspects of reality to be measured. Therefore, lifelogs gather only bits of information instead of providing an integrated overview of reality (Curry 2007; Del Giudice & Gardner 2009). Lifelogs are said to be intrinsically limited in capturing information (Dodge & Kitchin 2007). They only gather empirical information; they are unable to capture subjective experience. Other sources also mention the impossibility of capturing context in which information gets its meaning (Bannon 2011; Del Giudice & Gardner 2009).

In addition, the idea of 'memory retrieval' is questioned (Bannon 2006; Curry 2007; Van Dijck 2005; Van Dijck 2012; Moreno 2004; Nack 2005; Sellen & Whittaker 2010). Memories are dissimilar to data, as they are subjective revisions of the past. In contrast to a photo, which is taken once at a certain point in time, a memory is constructed whenever it is prompted. This process differs at given times, hence the memory changes. Correspondingly, 'the sharing of experiences' seems equally farfetched: because experiences are subjective interpretations the genuine sharing of any experience might be/is impossible (Del Giudice & Gardner 2009). In contrast, some consider the ability of lifelogs to mirror reality of lesser importance than their effect on [perceptions of] representation and temporality, because an absolute distinction between objective reality and subjective interpretation is troublesome (Dib 2012).

3.2.1.4 Impeding forgetting

The desirability of one of the objectives of lifelogs, namely the capturing of events of a person's life, can be questioned because forgetting can be important (Allen 2008; Bannon 2006; Bannon 2011; Byrne, Kelly & Jones 2010; Clowes 2012; Van Dijck 2012; Dodge & Kitchin 2007; Dodge 2007; Van Den Eede 2011; Koops 2011; Murata 2011; Nack 2005; Sonvilla-Weiss 2008). Various reasons support this line of thinking. For instance the 'clean slate' argument: it should be possible to forget the past to allow persons to move beyond their past deeds (Koops 2011). This also has positive societal effects. For example, expunging records, such as financial and criminal records, can have a positive effect on productivity, as they limit one's eligibility for loans and jobs. Secondly, forgetting aids self-development because people should be able to change their opinions without this change being held against them (Koops 2011). In a broader sense, people could feel limited by the constant awareness of the possibility of their deeds being remembered at all times (Koops 2011). Thirdly, the recalling of events could impair reconciliation between people. Again this has societal implications as shown in South Africa with the establishment of the Truth and Reconciliation Commission in 1995 after Apartheid (Bannon 2006). Fourthly, non-forgetting might not be the enhancement one would hope for; the influx of memories could render one apathetic while the details obscure one's potential for abstract thought (O'Hara 2010a). Also, forgetting is an intrinsic part of controlling one's memory. Lifelogs would trigger memories one would prefer were forgotten (Murata 2011). Subsequently, one loses control of one's life story as one cannot choose what to forget (Clowes 2012; Murata 2011). After all, one is unable to choose which information is used and which left unused. Furthermore, non-forgetting could

hinder intellectual growth. Data of past behaviour might be used to personalise services which might be based on previous behaviour (Murata 2011). By doing so, they confirm and/or establish past and/or current behaviour. A final critique is more abstract. It holds that biological and technological memory are interwoven making it difficult to separate them. Moreover, both storing *and* deleting personal information, i.e. remembering or forgetting, will have an intricate effect, both good as well as harmful to an individual's memory, and society which one may not always notice (Van den Eede 2011). Therefore one has to critically assess both the merits of remembering/storing and forgetting/deleting.

3.2.1.5   Uncertainties

The current early developmental stage of lifelog evolution poses challenges because there are variables which limit one's ability to assess the consequences of the technology once it is used by individuals. The inability to legally regulate the technology completely before it has fully developed is an example of such a challenge. Thus, it remains unclear how stakeholders, such as companies, authorities, or fellow citizens, are legitimately allowed to use the technology (Allen 2008; Bell & Gemmell 2009; Cheng, Golubchik & Kay 2004; Dodge 2007; Bailey & Kerr 2007; Del Giudice & Gardner 2009; Koops 2011). The uncertainty about regulation also obscures the functioning of a technology in society (Bailey & Kerr 2007). There are further reasons why the functioning of a lifelog is uncertain: the control one has over the functioning of a lifelog and the information it produces (Bailey & Kerr 2007; Dodge & Kitchin 2007; Dodge 2007); the influence of a lifelog on identity (O'Hara 2010b; Clowes 2012; Moreno 2004); the interplay between biological memory and the lifelog (Clowes 2012). These variables can pose challenges to users and developers, but as yet it is uncertain if they will.

3.2.1.6   Impairing social interaction

Social interaction can be negatively affected by lifelogs (Allen 2008; Bell & Gemmell 2009; Murata 2011; O'Hara et al. 2006; O'Hara, Tuffield & Shadbolt 2009; O'Hara 2010b; Sonvilla-Weiss 2007). The disappearance of face-to-face encounters, i.e. the disappearance of a physical human presence in obtaining and spreading information has to be faced (O'Hara et al. 2006; O'Hara, Tuffield & Shadbolt 2009; O'Hara 2010b). Moreover, as mentioned, lifelogs could hinder social forgetfulness and thereby impair social bonds (Allen 2008; Murata 2011). Lifelogs will affect the existing set of social norms to the extent that it is likely it will require a redefinition of norms (Bell & Gemmell 2009; Sonvilla-Weiss 2008). A further challenge is that lifelogs lead to a decrease in particular human emotions when

dealing with others. People might become more dependent on lifelogs to memorise. In order to memorise, a lifelog will retrieve information without a social context or subjective experience. This loss might affect social interaction as this information is conveyed without human emotions as compassion and empathy. As a result, society as a whole could develop characteristics similar to autism or schizophrenia because its members use this dehumanised information for interaction (Murata 2011). Finally, the disappearance of others and the replacement by lifelogs as the source of information, which leaves less space for subjective interpretations, might influence one's identity (Murata 2011). The result is that lifelogs can affect or change who one is or perceives to be.

3.2.1.7   Psychological and health risks

Lifelogs have been ascribed possible negative effects on health. Some mention cognitive laziness (Del Giudice & Gardner 2009): people will not use their own memory but rather rely on their lifelogs. This could harm the capacity to remember. The human brain is malleable, it adjusts to external conditions. When parts of the brain are left unused they might lose their functionality. This way, an artificial memory is not necessarily an enhancement of the brain, because it could possibly reduce biological memory (Murata 2011). In addition, a technological rather than a biologically or socially constructed personal identity or awareness of the self might lead to autism or schizophrenia (Murata 2011). Another challenge is a lifelog being the cause of pathological rumination by facilitating ponderings for sufferers from bipolar and unipolar depression (Allen 2008; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011). Also, the recalling of events can be harmful. If, for example a memory of the event that led to a post-traumatic stress disorder were carelessly evoked, it could lead to a deterioration of the disorder (Allen 2008).

3.2.1.8   Issues concerning the protection of research subjects

'The protection of research subjects' is the only challenge that takes trials into account (Byrne, Kelly & Jones 2010; Price 2010b; Kelly et al. 2013; Sweeney 2004). This challenge has not been elaborated except in Kelly et al. (2013) who discuss an ethical framework for doing trials with wearable cameras. They advance an elaborate account of ethical challenges brought forward by lifelogging. The other sources only mention the problem without specifying it.

3.2.2 Opportunities

Table 4 shows the number of sources from the literature survey which identify a particular opportunity. I distinguished 6 opportunities which I will elaborate on in decreasing order of frequency in which they occur in the academic debate. The difference between the number of challenges (101) and opportunities (30) is not necessarily an indication of widespread adversity towards the further development of the field. In fact, some challenges are identified to streamline the development and integration. Smith, O'Hara & Lewis (2011), for example identify more challenges than opportunities although they propose lifelog software.

Opportunities	Occurrence
Citizen Empowerment	10
Personalised services	8
Valuable information	6
Health benefits	3
Behaviour modification	4
Shaping identity	1

Table 4: Overview of opportunities

3.2.2.1   Citizen empowerment

Lifelogs may empower citizens against undesirable behaviour of the authorities. Many sources mention sousveillance: citizens monitoring the authorities (Allen 2008; Bell & Gemmell 2009; Mann 2004a; Mann 2004b; Mann 2005a; Mann 2005b; Mann, Fung & Lo 2006; O'Hara, Tuffield & Shadbolt 2009; Rawassizadeh 2011; Weber 2010). Sousveillance is a reversal of surveillance in which the authorities watch citizens. Mann, who coined the term, broadly interprets it as both the secret taping of police brutality as well as questionnaires from the management handed to shoppers about their staff (Mann 2002). This latter example is in-band sousveillance and organised within an organisation. Relevant to lifelogs is out-of-band sousveillance. This is sousveillance by people outside the organisation. Lifelogs could record the behaviour of the authorities. These records can be shared. This way, the authorities are better controlled, because behaviour by officials is increasingly made visible.

Equiveillance, balancing surveillance and sousveillance, is another opportunity identified by Mann. This concept seems to entail that the adverse effects of surveillance would be cancelled out by sousveillance (Mann 2004a). A related opportunity is the ability to provide information about one's innocence to the authorities to refute accusations (O'Hara, Tuffield & Shadbolt 2009).

3.2.2.2 Personalised services

By using lifelogs, data software can be developed to increasingly accommodate the needs of specific users or groups, such as aids to memory, information retrieval, recommendation systems, educational tools, research tools, policy information, organisational information, information for historical studies (Bell & Gemmell 2009; Kang et al. 2011; Mann 2004a; Mann 2004b; Mann 2005a; Mann, Fung & Lo 2006; O'Hara, Tuffield & Shadbolt 2009; Rawassizadeh 2011).

3.2.2.3 Valuable (non-medical) insights

Lifelogs offer valuable information as well as valuable emotional information (Allen 2008; Bell & Gemmell 2009; Kang et al. 2011; Mann 2004b; Nack 2005). Lifelog data can serve to reflect on oneself or society as a whole, thereby gaining deeper personal or collective understanding. Increased self-understanding by lifelog information can positively influence self-control (Hall, Johansson & de Léon 2013). Mann (2004b) considers lifelogs to have artistic potential producing art and culture. Finally, the development of lifelog technology itself could also provide valuable information as it incites a rethinking on what constitutes a human being (Nack 2005). Also, it could gather or conserve emotionally valuable information about a loved one (Bell & Gemmell 2009).

3.2.2.4 Health benefits

Lifelogs might benefit health or improve medical practice. A case in point is the improvement of therapeutic tools (Allen 2008; Bell & Gemmell 2009; O'Hara, Tuffield & Shadbolt 2009). The ability to measure the patient's behaviour could lead to better diagnoses, improved therapies and beneficial lifestyle changes (Bell & Gemmell 2009). Another opportunity is telemedicine (O'Hara, Tuffield & Shadbolt 2009). Physiological signals do not necessarily have to be measured in the hospital, which makes it possible to provide some medical assistance from a distance, thereby enhancing patients' independence (O'Hara, Tuffield & Shadbolt 2009). Moreover, the vast amount of information one might collect from subjects could be used to improve medical studies (Bell & Gemmell 2009).

3.2.2.5 Behaviour modification

By increasing knowledge about their behaviour and feeding back this knowledge which is derived from lifelogs, people may improve their performance at some task (Rawassizadeh 2011) or change their behaviour to their benefit. Also, lifelogs could play a role in the prevention of criminal behaviour. The threat of being visible may make criminals think twice

before committing a crime (Allen 2008; Bell & Gemmell 2009). There is also a more abstract discussion about the interplay between organic memory and artificial memories in the sense of lifelogs in which it is suggested that lifelogs may extend the mind i.e. lifelogs would be considered a part of the human mind (Clowes 2013). This may be defined as a phenomenological position on lifelogs.

3.2.2.6 Control of identity

Identities can be constructed and imposed more easily as a consequence of using lifelogs. Some are constructed formally by authorities such as one's financial profile or identity card data and some informally by, for example a friend's views as to one's trustworthiness. The concept of identity, as used by O'Hara, Tuffield and Shadbolt 2009, in this sense is quite thin. It consists of certain properties and characteristics ascribed to the individual by another entity which can use this information. A lifelogger has more control over those externally imposed identities. The lifelogger could have a vast database of information which could be used to create a new identity or to oppose identities that have been ascribed to oneself by others. Without lifelogs, one would have less information at one's disposal to do this (O'Hara, Tuffield & Shadbolt 2009).

3.3 Discussion

As the results section showed, the debate around ethical issues offers an interesting discussion on a rich variety of challenges and opportunities concerning lifelogs. However, there are still important ethical issues, which have been neglected in the literature so far and need further analysis: (1) freedom, (2) decision-making, (3) imposed identities, (4) health and environment, (5) corporations, and (6) the choice of keeping lifelogs.

3.3.1 Liberty

Currently the discussion about the freedom of citizens in conjunction with lifelogs is mostly narrowed down to the relationship between state and citizens. Either the position of citizens is seen as strengthened by sousveillance, or lifelogs are regarded as an undesirable source of information available to governmental institutions to control its citizens. This, however, is too narrow a scope. Other aspects such as self-surveillance by officials and the relationship between citizens amongst themselves have to be taken into account as well.

3.3.1.1 Self-surveillance by officials

There is no reference to the self-surveillance of soldiers or other officials in the current literature, even though programmes such as the aforementioned DARPA project ASSIST and LifeLog (DARPA 2010; DARPA/IPTO 2003) shows a clear interest in lifelogs by governmental authorities. Besides providing the military with better information and possibly saving soldiers' lives, lifelogs could also strengthen the rights of citizens. Leaked information such as the abuse in Abu Ghraib and the US attack killing two Reuters' staff members brought to light misconduct.[23] Moreover, authorities can gain support by providing transparency.

Surprisingly, opportunities to combat crime by governmental institutions holding lifelogs of its citizens are left unmentioned although this opportunity was already brought forward when TIA was proposed and might be referred to again. Either way, citizens holding lifelogs and handing over information, or authorities accessing or holding lifelogs, could also enhance national security.

3.3.1.2 Questioning sousveillance

In order for lifelogs to become an emancipatory force there are challenges to overcome. The current ability of a lifelog to enhance the position of people vis-à-vis governmental organisations, as proposed by authors mentioning sousveillance, is not self-evident. This has various reasons of which some can be solved by improving technology while others can be solved through regulation. Firstly, sousveillance has only a limited reach: important areas of power will remain obfuscated, such as prisons, courtrooms, parliaments, backrooms and the way governmental institutions process and gather their data. Secondly, the increased visibility of citizens' dissatisfaction actually empowers the authorities. Governmental institutions will obtain insight into potential discontent at an early stage and can subsequently act on this information (Morozov 2011). Thirdly, Internet anonymity is often ill-protected, leaving the sharer of information vulnerable (Morozov 2011). Indeed, some governmental organisations have legal instruments that enable them to regulate or incite the development and use of information and communication technology, e.g. they could require backdoors in software to access data or hidden identifiers. This is arguably already the case with Skype and Facebook (Zetter 2012). This is an addition to the legal instruments they sometimes have to censor information. Fourthly, the information is shared by sources, i.e. common people, who have

---

[23] For more information on the attack on Reuters' staff: http://www.collateralmurder.com/

not yet been established as reliable news sources. Without verification, the information is more vulnerable to being discredited or ignored. A fifth issue is that it is doubtful that information is neither sufficient nor necessary to mobilise a movement (Morozov 2011). Information about governmental misbehaviour does not necessary lead to corrective action by citizens. Information alone does not satisfy the conditions necessary to improve the position of citizens vis-à-vis authorities, e.g. an organised resistance might be needed as well.

3.3.1.3 Little Brother

More power relations are affected by lifelogs than the relationship between governmental institutions and citizens. Another challenge to citizens' freedom is what Bell & Gemmell (2009) have aptly labelled 'Little Brother', i.e. citizens would enforce norms on each other. According to Foucault (1991), the constant threat of being monitored is sufficient to alter behaviour given that in most situations it would be unclear if one's behaviour is being recorded. This uncertainty makes conforming to social norms a prudent disposition which is problematic as social norms can be ethically undesirable. With lifelogs, citizens can spread a vast amount of information about others. The information can be used within a selected group of people, e.g. the family, or shared on platforms available to virtually all. Already, there are signs of ferocious social control with countless websites offering a platform to show photos and videos of people acting in discordance with existing social norms. Lifelog information can be shared as a curiosity but also with more harmful intentions, e.g. stories about photos circulating online as a revenge for a broken relationship or bullying tactic are readily available. In China there are 'human-flesh search engines' which are online searches to identify and punish an individual in real life who provoked the anger of an online community (Downey 2010). One of the victims killed a kitten on video. People have lost their jobs and/or needed to move home because of these raids into their privacy. This challenge is different to the one mentioned previously in which citizens figured as recreational spies. This social control is being executed by society without the interference of governmental institutions although it is regulated by legislation by restricting the sharing and accessing of information. Also this functioning is not necessarily harmful as people would feel more inclined to act according to established standards of decency, but has the potential to be harmful as social norms can be unjustifiable rigid and/or ethically undesirable. Moreover, the preventive effect ascribed to lifelogs of citizens watching each other seems reasonable (Allen 2008; Bell & Gemmell 2009). Therefore, it is also necessary to consider the security and safety provided by lifelogs.

3.3.1.4   Questioning transparency

There is still one challenge to be solved when discussing the freedom of people. The premise that transparency is beneficial is not necessarily valid. First of all, one simply does not have the resources or time to place all information in a correct frame which is particularly troublesome when lifelogs provide so much information about so many people. Therefore, if it is not contextualised even correct information can lead to a distorted image of the state of affairs (Lessig 2009). This is worsened as the rationale behind some acts is only apparent in a context. For example, sometimes one has no option but to choose between two wrongs (Nagel 1972). This has been labelled the 'dirty hands dilemma' in politics (Nagel 1972). Outside the context, the act might appear unjust. Secondly, a great part of politics, and arguably social life, is negotiating. These negotiations need a level of obscurity, because negotiators need the opportunity to distance themselves from losses. If this space is not provided, negotiations could be led into deadlock (Schrott & Spranger 2006, 6-7). Therefore, it is hard to defend transparency as unconditionally beneficial. Instead, one needs to critically assess the merits and disadvantages of transparency against the backdrop of the specifics of particular situations.

3.3.2   Decision-making

Lifelog information will have a considerable influence on how one perceives oneself and others and, subsequently, the decisions one makes. Exactly this ability has been one of the main reasons to develop lifelogs. Unfortunately this ability also raises challenges.

One of the fundamental assumptions behind lifelog technology is that the availability of its information leads to better decision making. One of the values of Western culture is, after all, the concept of intelligent choice, which means that one should be fully informed so as to be able to make intelligent decisions (Feldman & March 1981, 177). The ability to refer to information provides a justification and meaning for one's choices. Information has, for that reason, symbolic value that cannot be underestimated. Hence, it would be unlikely that this lifelog data has no influence on decisions in daily life.

This influence is not morally neutral. A device has normative standards built in, which are not necessarily explicated: in order to sell, information is framed in a way which is acceptable to most; technology has to comply with regulations and (political) standards; and the developers interweave their own values in design. Moreover, the manipulation of information can be profitable. For instance, a company developing medical products might be

inclined to stress the health aspects in events of someone's life and/or might emphasise minor deviations from health averages. The extent to which lifelogs influence beliefs has an effect on the responsibility of developers to explicate the built-in normative standards and to represent information fairly. This responsibility is greater as their influence becomes more significant.[24]

The extent to which lifelogs are able to influence convictions and actions is largely unknown. The concept of cognitive dissonance provides more insight into the possibilities of a lifelog to manipulate behaviour and/or beliefs. Imagine the following scenario: you eat crisps lying on the couch and are watching comedy shows on the television while information from your lifelog indicates you should exercise more and eat healthier because you consider your time to be valuable, your health important and lifelog information to be true. Cognitive dissonance, the existence of contradictory sets of beliefs, occurs here. This conflict provides a feeling of discomfort as one seeks consistency in one's convictions (Festinger 1962, 2-7). There are three ways to go about addressing this conundrum: (1) change one's actions, (2) change one's beliefs, or (3) find other elements that soften the conflict such as the addition of other sources of information. These solutions could prove difficult, as one incidentally might feel an emotional need to do little and eat unhealthily. As a result lifelogs could either create feelings of discomfort to the user or they could change one's actions and/or beliefs. Developers have to be sensitive to emotional needs as they influence the beliefs and actions of the holders. Finally, the ability to weigh everyday life decisions might actually complicate life for the individual user since responsibility can be attributed to innocuous, quotidian activities as they become increasingly visible.[25]

3.3.3 Imposed identities

I will use a thin conception of identity as was used by O'Hara, Tuffield and Shadbolt (2009). According to them an identity can consist of certain ascribed characteristics and properties which can be acted upon. Hence, one can have multiple identities. The information gathered on a passport can be considered an identity, but an identity can also be a financial profile or a public image. I will identify 3 challenges with lifelogs in relation to controlling one's identity.

---

[24] In case, lifelogs hinder memorisation, the dependency on a lifelog would be extreme. This dependency leaves companies and authorities with an even greater responsibility to provide sound information as they would heavily influence decisions.

[25] This shows some similarities to an issue with forms of utilitarianism in which one would have to consider every action in order to calculate utility. This is considered too cumbersome.

Firstly, timing and the ability to define information are important elements within social relations (Steinel, Utz & Koning 2010). There are various reasons why the ability to define information and timing are impaired by lifelogs. With regard to defining information, lifelog data are augmented with relevance and/or semantic meaning in order to gain an insight into one's life. The use of a lifelog would be very limited if it would just gather information. Imagine trying to wade through an unsorted photo album containing years of photos without any filtering. One would have great difficulties retrieving specific events. With regard to timing, the information others have about you has increased and therefore more information about you can be shared regardless of your preferences.

Secondly, the possibility of opposing identities can be questioned. To start, the opportunity to address an identity is dependent on the sharer or holder of the information. Some holders or sharers such as websites, authorities or companies offer no option to correct information. In other cases the information is proliferated in such a manner that the information cannot be corrected anymore. This can be especially troublesome if institutions such as governmental or financial institutions circulate wrongful information. In case of identity fraud, the spreading of false information without the necessary checks and balances could severely impair someone's opportunities as has happened.[26] Furthermore, one might have more difficulty reaching the same public. For instance, in a case of a public denouncement one might lack an equal platform to oppose statements. Also, content is not necessarily unequivocally available to all. The data a third party may have and the conclusions it inferred from it might be unclear. Moreover, the people or institutions holding, accessing or using your information might not be interested in a balanced depiction of the state of affairs associated with you and even if they do, they might lack the resources and/or capacity for doing this properly. In addition, it might be impossible to correct the created identity due to the nature of the information. For instance, the footage which portrays one as a lumbering drunkard cannot be rejoined with some evenings in which one was graceful and sober. Furthermore, the context might be deplorable as well. Although the behaviour might be acceptable and indeed common, one might have a reasonable inclination to distance oneself from being associated with it. Finally, as mentioned before, one has little control over the interpretation, editing and proliferation of information one shares (Bailey & Kerr 2007).

---

[26] This happened for example in the Netherlands with a business who was wrongfully arrested various times (ANP 2009). Somehow the databases could not correct the erroneous information. Identity fraud could either be facilitated by lifelogs, as one could steal more information, or impaired as one can hand over more information to correct the situation.

Thirdly, the ability to distance oneself from information is impaired. To begin with, through the Internet, information can be accessed irrespective of time and place. This leaves one with little ability to geographically distance oneself or to have one's past forgotten over time. In addition, identification techniques have improved. Data can be increasingly related to the person. This means that people who could not have been identified before can increasingly be identified on video and photos.[27] Moreover, the resources to proliferate and access data have decreased. The threshold has lowered to an extent that information about lesser known people is made available. Finally, it can prove almost impossible to remove data from the world-wide-web once it is released. These tendencies make it harder for someone to control their identity as the ability to walk away from past events is hindered.

3.3.4 Health and environment

In the coming century, urbanisation, pollution, scarcity of resources, affordable health care and the ageing world population are amongst the most pressing global concerns (Economist 2009; Economist 2010a; Economist 2010b; Siegele 2010). Most of these are alleviated by adjusting lifestyles and life patterns. For this, information that can be obtained by lifelogs which can mediate between personal, societal and/or global needs.[28]

For example, a yet unmentioned opportunity is that lifelog information could have significant impact in combating some of the most prevalent health issues, such as non-communicable diseases. These diseases include heart disease, stroke, cancer, diabetes, and obesity. Globally, 2 out of every 3 people die from these diseases (Beaglehole et al. 2011). They form a heavy burden on health care and cause poverty. Common causes are an overuse of dietary salt, physical inactivity, tobacco or alcohol abuse. Hence, those causes are related to lifestyles (Beaglehole & Yach 2003; Beaglehole et al. 2011; Ghaffar, Reddy & Singhi 2004; Hanson et al. 2011). Lifelogs provide insight into the life patterns of persons, which enables the signalling of unhealthy behaviour to prevent diseases. Also, diseases could perhaps be identified at an earlier stage, which would prevent costly latter stage interventions. Diagnoses might improve as well with the increase of information. Finally, people could gain more freedom from human assistance and gain more self-determination, since lifelogs could be used to monitor patients instead of staff. The ability to adjust life patterns may prove

---

[27] The body alone can be tracked using different properties, such as the ear, odour, heartbeat, voice, the iris, the periocular region, fingerprints, sweat, face recognition, DNA, and gait (Shachtman & Beckhusen 2013).

[28] Evidently, this will not help everybody as one should be able to afford the technology or have access to it.

equally beneficial in other areas of concern such as pollution as it could prevent energy wastage.

3.3.5 *Corporations as actors*

In the literature review carried out for this analysis of lifelogs, there is little written about the challenges that occur when corporations are entitled to hold or access lifelogs. [29] This is noticeable as the history of lifelogs shows a clear interest from companies to hold vast amounts of information about individual people. This poses various challenges and/or benefits as corporations can exert real influence.

Firstly, a corporation can exert real influence when owning or accessing lifelog content. For instance, when it can materially reward or penalise behaviour. Arguably companies such as financial institutions and insurance companies have this ability. In case of insurance companies, they could increasingly deter individuals from unhealthy behaviour with material penalties, by increasing premium costs or decreasing coverage. Although material deterrence of unhealthy behaviour can be desirable, it is questionable if insurance companies would be an appropriate agent. They could dictate lifestyles by too harshly penalising behaviour. Moreover, events from the past could show increased health risks which might jeopardise one's access to health care. Being held responsible could materialise in penalties such as higher insurance quotes as one could be required to show a responsible lifestyle. This happens currently with life insurances where smokers get higher quotes. Already, more seemingly benign information is harmful in a more general context as evidence suggests employers are currently judging prospective employees on online available content (De La Llama et al. 2012). Finally, challenges are posed when lifelogs are held by employers. Arguments in favour of this could be based on health, security and efficiency as employers obtain a better insight into the behaviour of employees. An issue is the freedom of the employee to consent. Also this could lead to surveillance as companies might start to regulate the behaviour of its employees too rigidly. Moreover, as previously mentioned, factual information does not necessarily prove sufficient to judge upon.

---

[29] Only Jayaram (2011) stresses the importance of privacy for businesses. Murata (2011) considers the issues with intellectual growth as companies have that much information to confirm previously established information. Del Giudice & Gardner (2009) consider the distance between management and staff if lifelogs are used. Others only briefly mention surveillance without much elaboration: Bailey & Kerr 2007; Del Giudice & Gardner 2009; Dodge & Kitchin 2007; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011; Sonvilla-Weiss 2008; Weber 2010.

A different issue is lifelog information being manipulated by companies. The lifelog could be used to create needs, e.g. pharmaceutical companies that use personal lifelogs to accentuate innocuous deviations in health or the cosmetic industry that use personal lifelogs to stress deviations from the beauty ideal.[30] Although people are already being influenced by the ubiquitous presence of advertisements which try to manipulate their view of the world or themselves, lifelogs leave the individual particularly vulnerable as the information directly relates to them. This leaves companies with additional responsibility to frame information in an acceptable way.

3.3.6 *The choice of keeping lifelogs*

With regard to the choice of keeping lifelogs in this domain of application, the information available from keeping lifelogs is focused upon first, which could profoundly impact daily life. Against this backdrop, concerns are explored about lifelogs kept by persons with reduced competence. Finally, the voluntariness of holding lifelogs is discussed.

3.3.6.1 **Impact of information available from keeping lifelogs**

To inform the holder of a lifelog about the kind of data stored and the parties that can access that data in the lifelog may prove difficult. As the access to lifelog data can negatively affect values such as one's privacy and liberty, clarity about access is important.[31] There are various reasons why this challenge is difficult to meet.

Firstly, it is impossible to assess what information can be obtained from data or technology over time. New information might be inferred from existing data by improving learning or retrieval techniques. Subsequently, data, previously considered harmless, could reveal undesirable information. For example, research has indicated that one's sexuality or political convictions can be inferred from a rudimentary source of information, such as (a part of) one's social network (Kosinski, Stillwell & Graepel 2013).[32] For this reason a distinction between private, sensitive data and public data is insufficient, since it is precisely the

---

[30] Even if companies refrain from manipulating data, the ability to measure bodily functions and behaviour facilitates comparisons and standards. Deviations in physical health or behaviour will become increasingly visible providing a feeding ground for neuroses and medicalisation.

[31] One is uncertain about how much of her privacy has been waived leaving one at risk if the data is ineffectively secured, handled sloppily, used for malign purposes, or shared with commercial or surveillant intentions. This concern is heightened if the information depicts a faulty state of affairs or if the information inferred from the data is false.

[32] Even mental states such as mental illnesses or undesirable character traits, such as narcissism and/or social anxiety, can be identified from posts on websites (Fernandez, Levinson & Rodebaugh 2012; Golbeck, Robles & Turner 2011; Mehdizadeh 2010).

feasibility of this distinction which is doubtful.[33] Thus, one is unaware of just how much privacy one has forfeited. This can have real life effects as third party access to information can influence one's opportunities in life, for example one's chances of employment or personal relationships with others.

Secondly, due to the complexity of lifelogging devices, clarity about data produced or shared is lacking. The smartphone, which seems set to become a pivotal lifelogging device, can serve as an example. It is difficult to both assess which parties can access particular data from a particular smartphone and to assess what data is gathered from that smartphone. This is partly explained by security glitches even experts are unaware of or a lack of openness from developers regarding which information is stored in which files. Apple, for example has been accused of storing location data on the iPhone and iPad (Allan & Warden 2011).[34] In addition, third parties can mediate the functioning of the device. The software and hardware compatible with the smartphone quite effortlessly manipulates the gathering and access of information.[35] Establishing that other parties have or had access is also quite troublesome, because accessing and copying data can leave little or no trail to the common user. Transparency about access to data is an intricate, albeit important, challenge when designing lifelogs as it has an effect on privacy. This is all the more complex as third parties such as governmental institutions, corporations and others could benefit from obscurity. Finally, lifelogs might be integrated into the fabric of everyday life to the extent that its functioning goes unnoticed, as the paradigm of pervasive computing describes. This may leave bystanders but also the users themselves potentially unaware of being lifelogged.

---

[33] There are other relevant variables that complicate a distinction between public and private information over time. The lifelogger and the environment in which they lifelogged can change. The lifelogger or the person recorded may consider data captured in the past inappropriate and harmful at present. Moreover, the information stored in a lifelog can become outdated. Lifestyles, social positions, behaviour, and beliefs change. Lifeloggers might be unaware of these changes and lifelogs might not capture them. When opportunities to correct this information are lacking, this can lead to incorrect profiles. This proves especially troublesome if information is used or spread by the lifelogger or third parties, such as corporations, governmental institutions, and hackers with nefarious intentions. Moreover, the (symbolic) value of information changes, meaning that information might obtain different and unforeseen connotations over time (Rawassizadeh 2011). Previously accepted or unenforceable yet unhealthy behaviour at an early stage of life might be punished at a later stage, for example through higher insurance quotes, lowered coverage, or social exclusion.

[34] There are numerous examples of devices sharing and gathering information without people's knowledge; these are a random pick: a smartphone taking photos (Chen 2011); a smartphone with serious security issues (Diaz 2008); software sharing information without people's awareness or consent (Thurm & Kane 2010); a smartphone stores whereabouts even when location services are disabled (Valentino-De Vries 2011).

[35] External devices can be added by the user, such as camera lenses, heart monitor gear, and covers. These devices are accompanied by software.

3.3.6.2 Concerns about lifelogs kept by persons with reduced competence

Competence is the ability to comprehend information provided and deal appropriately with the consequences of decisions based on this information. Some vulnerable groups have a diminished capacity to do just this. For instance, children are usually considered less able to foresee the consequences of their conduct. Besides, it is questionable how much information on vulnerable individuals should potentially be available to third parties, since this information could be used for malicious purposes, such as extortion. Additionally, from a didactically justified point of view, it might be important for their personal and intellectual growth to make mistakes without those mistakes being recorded and stored indefinitely or important to escape from the idea of being watched at all times.

Nevertheless, lifelogs should not necessarily be limited to technological competent adults, since lifelogs could be beneficial for people with diminished or not yet fully developed competence such as children or young adults or other groups, such as the elderly, with lower rates of technological competence. For example, access to children's lifelogs could be very useful to their carers, who would have an additional instrument to oversee activities of daily living, such as eating habits or online activities, ultimately helping them lead a safe and healthy life. The benefits of lifelogs might be reaped while the harms are limited by carefully selecting the information necessary and by putting it in the appropriate form. For this reason, an assessment of the ethical desirability of various functions of lifelogs for people with various levels of competence to use lifelogs is needed. It is necessary to assess the kind of information and devices that are beneficial for a particular group and the appropriate form in which the information should be presented.

3.3.6.3 Voluntariness of holding lifelogs

Because the consequences of holding a lifelog can be far-reaching, the voluntariness of keeping a lifelog is important. Societal pressure to keep lifelogs as a sign of innocence has already been mentioned (Allen 2008) and there may however be other forms of societal pressure to keep lifelogs and share information. Firstly, lifelogs could become necessary to guard reciprocity. If only one party in a conversion owns a lifelog even an innocuous chat could be harmful or made harmful by editing when shared by the lifelogger. The lifelogger can benefit from having more information than the other. The same applies to institutions which may obtain more information about the individual than the individual itself has. After all, a third party could construct a lifelog of an individual without the individual holding a personal lifelog. This leaves the individual vulnerable to artificially imposed identities.

A second additional form of societal pressure is society commanding the use of lifelogs by embedding them in the social fabric. Lifelogs could raise evidence standards. In a society in which lifelogs are the norm rather than a rarity, one might be expected to be able to hand over more information. Similarly, detailed phone bills or photos with one's partner could serve as proof of a relationship when applying for official documents, such as citizenship. A related issue is that lifelogs might become necessary to protect oneself against the authorities. For instance, Hasan Elahi currently uses a rudimentary form of a lifelog to protect himself against the authorities after the FBI required him to provide information about his activities following his identification as a potentially dangerous individual (O'Hara, Tuffield & Shadbolt 2009; TED 2011). This usage seems to disregard a fundamental right, namely the presumption of innocence by shifting the burden of proof towards the suspect. The existence of lifelogs could facilitate this erosion of rights by alleviating the burden of creating this information.

3.4   Conclusion

The history of lifelogs so far shows a clear corporate and governmental interest in lifelogs. Moreover, there seems to be an interest of consumers as well. Although the technology is still at an early stage of development, there has been considerable ethical significance attached to the development of lifelogs.

First, an insight in the current ethical debate on lifelogs is provided by identifying challenges and opportunities. The terminology of challenges and opportunities has been chosen as it distinguishes clearly areas of opportunity and need. The identification of challenges and opportunities provides an instrument which could aid the further development of this technology. Some of these newly identified challenges and opportunities might arise from blind spots in the current debate regarding users and motivations. Whilst the current debate focuses mainly on lifelogs held by individuals, lifelogs held by governmental institutions and corporations pose idiosyncratic ethical concerns as well. The recent history of lifelogs creates an urgent need to scrutinise the consequences of those entities holding them.

Secondly, some areas of ethical interest are identified that have yet to be further developed according to this research. Despite the rich academic debate on lifelogs for private individuals, some challenges previously left untouched are identified with regard to lifelogs held by private individuals for reasons affecting lifestyle.

Bibliography

Allan, A. & Warden, P. 2011. Got an iPhone or 3G iPad? Apple is recording your moves [Online]. O'Reilly Radar. Available from: http://radar.oreilly.com/2011/04/apple-location-tracking.html [Accessed 15-01-2013].

Allen, A.L. 2008. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74.

Bailey, J. & Kerr, I.R. 2007. Seizing Control? The Experience Capture Experiments of Ringley & Mann. *Ethics and Information Technology*, 9(2), pp. 129-139.

Bannon, L. 2006. Forgetting as a Feature not a Bug. *CoDesign.* 2(1), pp. 3-15.

Bannon, L. 2011. Reimagining HCI: Toward a More Human-Centered Perspective. *Interactions*, 18(4), pp. 50-57.

Beaglehole, R., & Yach, D. 2003. Globalisation and the prevention and control of non-communicable disease: the neglected chronic diseases of adults". *The Lancet*. 362 (9387), pp. 903-8.

Beaglehole, R., Bonita, R., Horton, R., Adams, C., Alleyne, G., Asaria, P., Baugh, V., Bekedam, H., Billo, N., Casswell, S., Cecchini, M., Colagiuri, R., Colagiuri, S., Collins, T., Ebrahim, S., Engelgau, M., Galea, G., Gaziano, R., Geneau, R., Haines, A., Hospedales, J., Jha, P., Keeling, A., Leeder, S., Lincoln, P., McKee, M., Mackay, J., Magnusson, R., Moodie, R., Mwatsama, M., Nishtar, S., Norrving, B., Patterson, D., Piot, P., Ralston, J., Rani, M., Reddy, K.S., Sassi, F., Sheron, N., Stuckler, D., Suh, I., Torode, J., Varghese, C., & Wat, J. 2011. Priority actions for the non-communicable disease crisis. *The Lancet*, 377(9775), pp. 1438-1447.

Bell, G & Gemmell, J. 2009. *Total Recall: How The E-Memory Revolution Will Change Anything.* New York: Dutton.

Bell, G. & Gemmell, J. 2007. A Digital Life. *Scientific American*. Available from: http://www.scienceandsociety.org/web/Library_files/A.Digital.Life.pdf. [Accessed 28-05-2012].

Bush, V. 1945. As we may think. *The Atlantic Monthly,* 176(1), pp. 101-108.

Byrne, D, Kelly, L., & Jones, G.J.F. 2010. Multiple Multimodal Mobile Devices: Lessons Learned from Engineering Lifelog Solutions. In: Alencar P. and Cowan, D. 2012. *Handbook of Research on Mobile Software Engineering: Design, Implementation and Emergent Applications*, IGI Publishing.

Chen, B.X. 2011. Creepy Bug Gives Some iPhones Unwanted FaceTime [Online]. *Wired.com*. Available from: http://www.wired.com/gadgetlab/2011/04/creepy-iphone-bug/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29 [Accessed 23-05-2012].

Chen, Y. & Jones, G.J.F. 2012. What do people want from their lifelogs? *IN: 6th Irish Human Computer Interaction Conference*.

Cheng, W.C. Golubchik, L. & Kay, D.G. 2004. Total recall: are privacy changes inevitable? *Proceedings of the 1st ACM workshop on Continuous archival and retrieval of personal experiences*, pp. 86-92.

Clowes, R.W. 2012. Hybrid Memory, Cognitive Technology and Self. *The proceedings of the AISB and IACAP World Congress 2012.*

Clowes, R.W. 2013. The Cognitive Integration of E-Memory. *Review of Philosophy and Psychology*, 4(1), pp 107-133.

Curry, M.R. 2007. Being there then: Ubiquitous computing and the anxiety of reference. *International Review of Information Ethics*, 8(8), pp. 13-19.

DARPA. 2010. *Advanced Soldier Sensor Information Systems and Technology (ASSIST)* [Online]. Available from: http://www.darpa.mil/Our_Work/I2O/Programs/Advanced_Soldier_Sensor_Information_Systems_and_Technology_(ASSIST).aspx [Accessed 30-01-2012].

DARPA/IPTO. 2003. *BAA # 03-30 LifeLog Proposer Information Pamphlet* [Online]. Available from: http://realnews247.com/lifelog.htm [Accessed 30-01-2012].

De La Llama, V.A., Trueba, I., Voges, C., Barreto, C. & Park, D.J. 2012. At Face(book) value: uses of Facebook in hiring processes and the role of identity in social networks. *International Journal of Work Innovation*, 1(1), pp. 114-136.

Diaz, J. 2008. Huge iPhone Security Flaw Puts All Private Information at Risk [Online]. *Gizmodo*. Available from: http://gizmodo.com/5042332/huge-security-iphone-flaw-puts-all-private-information-at-risk [Accessed 30-01-2012].

Dib, L. 2008. Memory as Concept in the Design of Digital Recording Devices. Altérités, 5(1), pp. 38-53.

Dib, L. 2012. The Forgetting Dis-ease: Making Time Matter. *A Journal of Feminist Cultural Studies*, 23(3), pp. 43-73.

Dijck, J. Van. 2005. From shoebox to performative agent: the computer as personal memory machine. *New Media & Society*, 7(3), pp. 311-332.

Dijck, J. Van. 2012. *Mediated memories in the Digital Age*. Stanford: Stanford University Press.

Dodge, M. & Kitchin 2005. The ethics of forgetting in an age of pervasive computing. *CASA Working Papers 92*. London: Centre for Advanced Spatial Analysis.

Dodge, M. & Kitchin, R., 2007. Outlines of a world coming into existence': pervasive computing and the ethics of forgetting. *Environment and Planning B Planning and Design*, 34(3), pp.431-445.

Dodge, M. 2007. Do we need an ethics of forgetting in a world of digital 'memories for life'? *Position paper for Designing for Forgetting and Exclusion conference.*

Downey, T. 2010. China's Cyberposse [Online]. *The New York Times*. Available from: http://www.nytimes.com/2010/03/07/magazine/07Human-t.html?pagewanted=all&_r=0 [Accessed 08-01-2013].

Economist. 2009. Building the smart grid [Online]. *The Economist.* Available from: http://www.economist.com/node/13725843 [Accessed 30-01-2012].

Economist. 2010a. Living on a platform [Online]. *The Economist.* Available from: http://www.economist.com/node/17388308 [Accessed 30-01-2012].

Economist. 2010b. Making every drop count [Online]. *The Economist.* Available from: http://www.economist.com/node/17388318 [Accessed 30-01-2012].

Eede, Y. Van Den. 2011. Technological remembering/forgetting: A Faustian bargain? *Empedocles: European Journal for the Philosophy of Communication*, 2(2), pp. 167-180.

Feldman, M.S., & March, J.G. 1981. *Information in Organizations as Signal and Symbol. Administrative Science Quarterly*, 26(2), pp. 171-86.

Fernandez, K. C., Levinson, C. A. & Rodebaugh, T. L. 2012. Profiling: Predicting Social Anxiety From Facebook Profiles. *Social Psychological and Personality Science*.

Festinger, L. 1962. *A Theory Of Cognitive Dissonance.* Stanford: Stanford University Press.

Foucault, M. 1991. *Discipline and Punish: The Birth of a Prison*. London: Penguin.

Ghaffar A., Reddy, K.S. & Singhi, M. 2004. Burden of non-communicable diseases in South Asia. *BMJ*, 328(7443), pp. 807-10.

Giudice, K. Del. & Gardner, M. 2009. *The Message of the Pensieve: Realizing Memories through the World Wide Web and Virtual Reality.* Unpublished. Available from: http://web.mit.edu/comm-forum/mit6/papers/Delgiudice.pdf.

Golbeck, J., Robles C. & Turner K. 2011. Predicting personality with social media. *Conference on Human Factors in Computing Systems* - Proceedings, pp. 253-262

Hall, L., Johansson, P., & de Léon, D. 2013. Recomposing the Will: Distributed motivation and computer mediated extrospection. In: Vierkant, T., Clark, A. & Kiverstein, J. (Eds.). *Decomposing the will*. Oxford: Oxford University Press: Philosophy of Mind Series.

Hanson, M., Godfrey, K.M., Lillycrop, K.A., Burdge, G.C. & Gluckman, P.D. 2011. Developmental plasticity and developmental origins of non-communicable disease:

Theoretical considerations and epigenetic mechanisms. *Progress in Biophysics and Molecular Biology*, 106(1), pp. 272-280.

Heersmink, R., Hoven, J. Van Den, Eck, N.J. Van, & Den Berg, J. 2011. Bibliometric mapping of computer and information ethics. *Ethics and Inf. Technol*, 13(3), pp. 241-249.

Jacquemard, T., Novitzky, R., O'Brolcháin, F., Smeaton, A.F. & Gordijn, B. 2014. Challenges and opportunities of lifelog technologies: a literature review and critical analysis. *Science and Engineering Ethics*, 20(2), pp. 379-409.

Jayaram, M. 2011. The Business of Privacy: From Private Anxiety To Commercial Sense? A Broad Overview of Why Privacy Ought To matter To Indian Businesses. *NUJS Law Review*, 4(4), pp. 567-594.

Kang, J., Shilton, K., Estrin, D., Burke, J.A & Hansen, M. 2011. Self-Surveillance Privacy. *UC Los Angeles: UCLA School of Law*, pp. 1-43.

Katz, R.N. & Gandel, P.B. 2008. The Tower, the Cloud, and Posterity. In: Katz, R.N. (ed.), *The Tower and the Cloud; Higher Education in the Age of Cloud Computing*. Berkeley: EDUCAUSE.

Kelly, P., Marshall, S.J., Badland, H., Kerr, J., Oliver, M., Doherty, A.R. & Foster C. 2013. An Ethical Framework for Automated, Wearable Cameras in Health Behavior Research. *Am J Prev Med*, 44(3), pp. 314-319.

Koops, E.J. 2011. Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice. *SCRIPTed*, 8(3), pp. 229-256.

Kosinski, M., Stillwell, D. & Graepel, T. 2013. Private Traits and Attributes are Predictable from Digital Records of Human Behavior. *PNAS*, 110(15), pp. 5802-5805.

Lahlou, S. 2008. Identity, social status, privacy and face-keeping in digital society. *Social Science Information,* 47(3), pp. 299-330.

Lemos, A. 2011. Locative Media and Surveillance at the Boundaries of Informational Territories. In: Firmino, R., Duarte, F., & Ultramari, C. *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks*, IGI Publishing, pp. 129-149.

Lessig, L. 2009. Against Transparency: The perils of openness in government [Online]. *The New Republic.* Available from: http://www.tnr.com/article/books-and-arts/against-transparency?page=0,5 [Accessed 13-02-2012].

Mann, S. 2002. Sousveillance [Online]. *Wearcam.org.* Available from: http://wearcam.org/sousveillance.htm. [Accessed 05-04-2012].

Mann, S. 2004a. "Sousveillance" Inverse Surveillance in Multimedia Imaging. *MULTIMEDIA '04 Proceedings of the 12th annual ACM international conference on Multimedia,* pp. 620-627.

Mann, S. 2004b. Continuous lifelong capture of personal experience with EyeTap. *Proceedings of the the 1st ACM workshop on Continuous archival and retrieval of personal experiences*. ACM SIGMM. New York, NY.

Mann, S. 2005a. Sousveillance and cyborglogs. A 30-year empirical voyage through ethical, legal and policy issues. *Presence: Teleoperators and Virtual Environments*, 14(6), pp. 625–646.

Mann, S. 2005b. *Equiveillance: The equilibrium between Sur-veillance and Sous-veillance*.

Mann, S., Fung, J. & Lo, R. 2006. Cyborglogging with Camera Phones: Steps Toward Equiveillance. *Proceedings of the ACM Multimedia 2006*.

Mayer-Schönberger, V. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton: Princeton University Press.

Mehdizadeh, S. 2010. Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook . *Cyberpsychology, behavior and social networking*., 13(4), pp. 357-364.

Moreno, J. 2004. DARPA On Your Mind. *Cerebrum*, 6(4), pp. 92-100.

Morozov, E. 2011. *The net delusion: how not to liberate the world*. London: Allen Lane.

Murata, K. 2011. The right to forget/be forgotten. In: *CEPE 2011: Crossing Boundaries*.

Nack, F. 2005. You Must Remember This. *IEEE Multimedia*, 12(1), pp. 4-7.

Nagel, T. 1972. War and Massacre. *Philosophy and Public Affairs*, 1(2), pp. 123-144.

O'Hara, K., Morris, R., Shadbolt, N., Hitch, G. J., Hall, W. & Beagrie, N. 2006. Memories for Life: A Review of the Science and Technology. *Journal of the Royal Society Interface*, 3 (8). pp. 351-365.

O'Hara, K. & Hall, W. 2008. Trust on the Web: Some Web Science Research Challenges [Online]. *UOC Papers*. Available from: http://www.uoc.edu/uocpapers/7/dt/eng/ohara_hall.pdf [Accessed 13-02-2012].

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

O'Hara, K. 2010a. Narcissus to a Man: Lifelogging, Technology and the Normativity of Truth. E. Berry et al., eds. *Second Annual SenseCam Symposium*. Available at: http://eprints.ecs.soton.ac.uk/21904/.

O'Hara, K. 2010b. Arius in Cyberspace: Digital Companions and the Limits of the Person. In: Yorick Wilks (ed.), *Close Engagements with Artificial Companions: Key social, psychological, ethical and design issues*, Amsterdam: John Benjamins.

O'Hara, Kieron. 2012. The Technology of Collective Memory and the Normativity of Truth. In: Goldberg, D., McCarthy, N. & Michelfelder, D. (eds.) *Philosophy and Engineering: Reflections on Practice, Principles and Process*, Berlin: Springer-Verlag.

Price, B.A. 2010a. Towards Privacy Preserving Lifelogging. *Proceedings of the second annual SenseCam symposium.*

Price, B.A. 2010b. Challenges in Eliciting Privacy and Usability Requirements for Lifelogging. *Conference'10*.

Rawassizadeh, R. & Min Tjoa, A. 2010. Securing Shareable Life-logs. *The Second IEEE International Conference on Information Privacy, Security, Risk and Trust.* Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5590506.

Rawassizadeh, R. 2011. Towards sharing life-log information with society. *Behaviour & Information Technology*, pp. 1-11.

Schrott, A. & Spranger, D. 2006. Mediatization of political negotiations in modern democracies: institutional characteristics matter. *National Centre of Competence in Research (NCCR) Challenges to Democracy in the 21st Century, Working Paper No. 2*. Zurich: University of Zurich.

Sellen, A.J. & Whittaker, S. 2010. Beyond total capture: a constructive critique of lifelogging. *Communications of the ACM*, 53(5), pp. 71-72.

Shachtman, N. & Beckhusen, R. 2013. 11 Body Parts Defense Researchers Will Use to Track You [Online] Wired.com. Available from: http://www.wired.com/dangerroom/2013/01/biometrics/?pid=1775&viewall=true [Accessed 25-01-2013].

Siegele, L. 2010. It's a smart world. *The Economist* [Online] Available from: http://www.economist.com/node/17388368 [Accessed 21 December 2010].

Smith, A., O'Hara, K. & Lewis, P. 2011. Visualising the Past: Annotating a Life with Linked Open Data. *Web Science Conference 2011, June 14th-17th 2011, Koblenz Germany*.

Sonvilla-Weiss, S. 2008. *(IN)VISIBLE: Learning to Act in the Metaverse*. Vienna: Springer.

Steinel, W., S. Utz, & Koning, L. 2010. The good, the bad and the ugly thing to do when sharing information: Revealing, concealing and lying depend on social motivation, distribution and importance of information. *Organizational Behavior and Human Decision Processes*, 113(2), pp. 85-96.

Sweeney, L. 2004. Navigating Computer Science Research Through Waves of Privacy Concerns: Discussions among Computer Scientists at Carnegie Mellon University. *ACM Computers and Society*, 34(1), pp. 1-19.

TED. 2011. *Hasan Elahi: FBI, here I am!* [Online]. Available from: http://www.ted.com/talks/hasan_elahi.html [Accessed 23-05-2012].

Thurm, S. & Kane, I.Y. 2010. Your Apps Are Watching You. *The Wall Street Journal* [Online]. Available from: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html?mod=WSJ_hps_sections_tech [Accessed 23-05-2012].

Turkle, S. 2008. Inner History. In: Turkle, S. (ed.) *The Inner History of Devices.* Cambridge: The MIT Press.

Turkle, S. 2011. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books.

Valentino-De Vries. 2011. IPhone Stored Location in Test Even if Disabled [Online]. *The Wall Street Journal*. Available from: http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html?mod=WSJ_article_comments#articleTabs%3Dcomments [Accessed 23-05-2012].

Weber, K. 2010. Mobile Devices and a New Understanding of Presence. In: *Workshop paper from SISSI2010 at the 12th annual ACM International conference on Ubiquitous Computing*, p. 101.

Werkhoven, P. 2005. Experience machines: capturing and retrieving personal content. In: Bruck, P.A., Buchholz, A., Karssen, Z. & Zerfass, A. (eds.) *E-content Technologies and Perspectives for the European Market* New York, Heidelberg, Berlin: Springer.

Zetter, K. 2012. FBI Wants Backdoors in Facebook, Skype and Instant Messaging [Online]. *Wired.com.* Available from: http://www.wired.com/threatlevel/2012/05/fbi-seeks-internet-backdoors/ [Accessed 08-01-2013].

Being a lifelogger

4 Privacy

Introduction

Privacy is the ethical issue most frequently associated with lifelog technology in the academic debate presented above (*3.2.1 Challenges*). This is unsurprising, as lifelog technology facilitates the retrieval and distribution of personal information.

The aim of this chapter is to provide more clarity on the issue of privacy and lifelogs. Firstly, an account of privacy is provided, as it is a complex concept with multiple facets. Secondly, the manners in which lifelogs affect the privacy of lifeloggers and non-lifeloggers negatively are examined. Thirdly, an opportunity regarding the privacy of lifeloggers is discussed. Fourthly, extenuating circumstances that contextualise the above mentioned issues are identified. Fifthly, possible design recommendations are offered to address issues related to the privacy of lifeloggers and non-lifeloggers.

4.1 Concept of privacy

The definition of privacy is heavily debated, which leaves one without a definition of privacy about which there is a general consensus. The definition of privacy as posited here comes from the 'Restricted Access/Limited Control' (RALC) theory of privacy (Tavani 2007, 2), which combines elements of access and control as conditions of privacy. The benefits of such an approach become apparent after discussing accounts of privacy, which primarily focus either on 'access' or on 'control'.

4.1.1 Access based accounts of privacy

Two theories of access will be briefly discussed, the first is a non-intrusion account as posited by Warren and Brandeis (1890) and the other is a seclusion account as posited by Gavison (1980).

1) In 1890, Warren and Brandeis formulated their account of privacy as "the right to be let alone" (Warren & Brandeis 1890, 193). Their influential article on the right to privacy led to a more systematic discussion on the concept of privacy (DeCew 2013); a concept that was only implied in previous works by philosophers such as Aristotle (1984), Locke (1689) and Mill (1859). Their initiation of the discussion on the right to privacy influenced the legal debate on privacy in the US, and gave the legal framework to protect privacy its current form in which violations of privacy are considered a tort (Kalven 1966). Warren and Brandeis'

initial purpose was to show that the US common law recognises a right to privacy, and to examine the scope and nature of that right (Warren & Brandeis 1890, 206). According to them, a right to privacy would allow people to protect themselves against unwanted intrusion; a need that arose because they perceived a tendency by the media to fail to adhere to the norms of "propriety and decency" (Warren & Brandeis 1890, 196). Technological developments, including recording devices, were at the heart of their concern, as they mention "the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds" (Warren & Brandeis 1890, 206).

Moor (1990, 71) argues that Warren and Brandeis' account of privacy is unsuccessful in capturing commonly held intuitions concerning privacy. On the one hand, their definition is too narrow, as it fails to include some acts which one would typically consider to be a violation of privacy. For example, someone who would merely search through another person's files, such as bank statements or love letters, but would leave the information he gains unused for whatever reason, would not infringe the other person's privacy, as he would let that person alone. Typically one would consider these acts to violate privacy. On the other hand, their definition is too broad, and could include acts which one would ordinarily *not* consider to be violating privacy. For example, any passer-by on the street who asks for directions could be said to violate privacy, but one would ordinarily not consider this a violation of privacy (Moor 1990).

Another concern is that, according to Moor (1990), Warren and Brandeis' account fails to distinguish properly between liberty and privacy. The right to privacy and liberty are distinctive rights. If the two are not properly distinguished from each other, a risk is created that privacy becomes a trump to shield harmful actions; a domestic abuser should not be able to defend herself by claiming that the right to privacy extends to her being free to act without being intruded upon. One may have certain rights to privacy within the household, but one has no right to abuse one's partner (Moor 1990, 74). By defining the right to privacy as the right to be let alone, this distinction between liberty and privacy is lost and one could argue that, based on this definition, the right to privacy is a right to freedom.

2) Gavison offers a different account of privacy based on seclusion. She defines privacy as inversely correlated with "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention" (Gavison 1980, 423). Commenting on Gavison, Tavani (2007) argues that

70

she succeeds in distinguishing privacy from liberty by defining privacy in terms of seclusion rather than freedom from intrusion. Moreover, he acknowledges that the ability to hide or reveal personal information seems inherent to privacy (Tavani 2007).

Nonetheless, accounts focusing on seclusion fail to capture all aspects of privacy. Most importantly, they fail to capture the importance of control and seem to confuse privacy with secrecy (Tavani 2007, 9). Indeed, according to Gavison, "an individual enjoys perfect privacy when he is completely inaccessible to others" (Gavison 1980, 428). These accounts of privacy, however, seem to undervalue the importance of control and confuse privacy with secrecy. One could conclude that one enjoys perfect privacy on a deserted island following Gavison (Tavani 2007). However, one could question if one has privacy in any meaningful way in such a desolated place. The importance of control can be illustrated with an example. Suppose a patient discusses private matters necessary for her medical treatment with medical staff. The patient is commonly thought to have social, moral and legal rights to privacy that the medical staff should respect. Her privacy may have been diminished when examined by the doctor, but no rights to privacy seem to have been violated. In fact, there are strict limitations in place to the sharing of medical information to protect the privacy of patients. A patient's rights to privacy are safeguarded by norms and regulations that allow her to choose to whom to reveal her information. After all, the patient might only feel inclined to reveal her personal information or allow access to her body, if she is competent to decide at all, because she has sufficient assurance that her right to privacy will be respected. In this example, the meaningfulness of privacy was primarily determined by the ability to control the access of information rather than by the kind of solitude one would experience on a deserted island. Hence, privacy not only seems determined by inaccessibility, but privacy also implies control over the disclosure and flow of information.

4.1.2 Control based accounts of privacy

The second type of account defines privacy by access. Examples are Fried's (1968) and Westin's (1966) accounts of privacy. Fried states that "[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves" (Fried 1986, 482). Westin defined the right of individual privacy as "the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public" (Westin 1966, 1031). These accounts have important advantages. The distinction

between liberty and privacy is made, because, according to these accounts, privacy is not the same as being free from intrusion (Tavani & Moor 2001). Furthermore, the idea that people can choose to disclose or hide information seems in line with moral intuitions that are commonly held about privacy (Tavani & Moor 2001). Some weaknesses are, however, associated with control based accounts of privacy.

One counterintuitive consequence of defining privacy as control is that the scope of what can be private is greatly reduced (Tavani & Moor 2001). If privacy is defined by control, one would *de facto* have little to no privacy, even at times when one would consider oneself to experience privacy (Moor 1990). For instance, the existence of databases storing personal information outside the control means that there is little information one does control (Tavani & Moor 2001). However, if personal data are used properly, or not at all, these databases may not violate privacy (Nissenbaum 2004a). For example, birth registers contain a massive amount of personal information which is stored out of people's control. These databases may be considered a potential threat to privacy, for example when they are breached, but these databases do not violate or negate privacy *per se*. In addition, equating privacy with direct and personal control over personal information means that once one shares a piece of information about oneself, one has effectively forfeited one's privacy as one may have no control over what the other does with this information (Moor 1990). However, often information is shared without violating privacy, and, indeed, in compliance with regulations for the protection of privacy. Tavani and Moor (2001) mention another counterintuitive consequence of equalling privacy with control: it implies that when one is physically unable to control personal information, one loses one's privacy. However, it seems that one keeps some rights to privacy even under anaesthesia, or (temporarily) lacking the competence to control one's personal information otherwise (Tavani & Moor 2001, 6-7).

4.1.3 Restricted Access/Limited Control

Though both control and access based accounts of privacy have advantages, they are insufficient by themselves. Therefore, Tavani and Moor have advanced the RALC theory of privacy (Moor 1990; Moor 1997; Tavani & Moor 2001; Tavani 2007; Tavani 2008)[36,37]

---

[36] The RALC theory of privacy consists of three different elements: (1) a definition of privacy, (2) an account of the management of privacy, and (3) a justification for respect for privacy (Tavani & Moor 2001; Tavani 2007, 10; Tavani 2008, 163). Moor called it the 'Control/Restricted Access' theory (Moor 1990; 1997). However, this new account is referred to by Tavani (2007) as the "Restricted Access/Limited Control (RALC) theory of privacy" (Tavani 2007, 10-11). In this dissertation, the latter terminology will be used, because Moor indicated he was unhappy with his own initial label, and agreed with the name provided by Tavani (Tavani 2007).

which combines elements of both theories so as to avoid their weaknesses and exploit their advantages.

The RALC theory uses the following definition of privacy: "[a]n individual or group has normative privacy in a situation with regard to others if and only if in that situation the individual or group is normatively protected from intrusion, interference, and information access by others" (Moor 1997, 30). Moor intentionally uses the broad term 'situation' so that privacy could cover miscellaneous topics such as locations, activities and relationships (Moor 1997, 30). The term 'situation' also allows one to vary the level of detail to describe the circumstances in which privacy is applied. In this dissertation, the 'situation' is shaped by lifelogs for members of the general public for private purposes such as the one used in the scenario (*2.5 Scenario*), but the situation could be defined in a narrower sense, for example with regard to lifelogging by private individuals for purposes of leisure but only in public places, or the situation could be defined in a broader sense, for example with regard to lifelogs for organisations and individuals.

The RALC theory distinguishes a right to privacy from the conditions that one needs to experience privacy. In the definition the term 'normative' is mentioned, which implies that one can have non-normative privacy as well (Moor 1997). Indeed, Moor distinguishes between naturally private situations and normatively private situations (Moor 1990). The distinction between naturally and normatively private is a distinction between descriptive, stating the conditions to experience privacy, and normative, stating that there are rights to protect privacy are in place (Tavani 2007, 10). According to Tavani and Moor, these rights stem from social conventions, ethical and legal considerations that justify claims to privacy (Moor 1997; Tavani & Moor 2001, 7). To further clarify this distinction, Moor (1997) provides the example of a family walking through a publicly accessible forest. They experience privacy because they are out of the sight of other people. The moment a group of scouts see them, they lose their privacy. Nonetheless, one can hardly maintain that these scouts are *violating* their privacy as the family did not have the right to not being seen in the forest. Being seen by scouts *reduces* or *diminishes* the family's privacy, but the scouts do not necessarily violate their right to privacy. One violates privacy when one reduces privacy where the other person has a right to privacy that should have been respected. Again,

---

[37] Moor (1990) first advanced this new account of privacy. Moor's and Tavani's conception is similar. Tavani often expands on or reformulates Moor's arguments. This may sometimes be confusing to the reader who finds references to Tavani when the original argument came from Moor.

following Moor's (1997) example, if the scouts would enter the family's house uninvited this would most likely constitute a violation of privacy. People are commonly expected to have some claims to privacy in their home, as there are social, legal, and moral norms that forbid others to enter their houses without their permission. The definition used by the RALC theory echoes access accounts of privacy in which the rights to privacy depend on the context in which information is accessed. The control element to privacy will be discussed below (*4.1.5 Control and privacy*).

4.1.4 Normatively private situations

Nissenbaum (1998 & 2004a) makes a distinction between normatively and naturally private situations similar to the one made by Tavani and Moor, and her account will be offered to explain the concept of a normatively private situation in more detail. The explanation offered by Tavani and Moor seems to go little beyond mentioning that normatively private situations are defined by social, legal, and moral norms.

According to Nissenbaum, normative claims to privacy are determined by "contextual integrity" (Nissenbaum 1998, 559). Her use of the term 'context' is similar to the term 'situation', as used by Tavani and Moor. According to Nissenbaum, norms are always applicable, which set limitations on information flows (Nissenbaum 2004a, 121).[38] Thus, the popular conception that in public there is no privacy is misguided: for example, although during an encounter in the supermarket it is acceptable for a neighbour to see the groceries in one's shopping cart – people can usually see what is inside the cart, and commonly people have no problem with this being so -, it may be inappropriate or unjust if the same neighbour posts videos of one's shopping behaviour online, or if the supermarket offers information about the shopping of individual customers online.[39] Following Nissenbaum, the applicable norms are dependent on the context – the characteristics of the context determines the norms applicable (Nissenbaum 2004a, 123). She identifies two sets of norms that regulate the disclosure and revelation of information. Violations are determined by non-compliance with

---

[38] The scope of norms regulating privacy is broad, "potentially extending over information, activities, decisions, thoughts, bodies, and communication" (Nissenbaum 2004a, 105). In this vein it is possible to incorporate various other accounts of privacy such as physical privacy distinguished by Allen (2011). However, the scope of this inquiry is mostly limited to informational privacy.

[39] Reiman (1995) offers a factual remark which supports this claim: by monitoring the public life of an individual, detailed information about his private life will be obtained as one might gain insight into his religious beliefs, his social network, his health, his pastimes, etc.

norms relating to (1) appropriateness and (2) distribution. This set of norms allows one to distinguish between normatively and naturally private situations

1) The set of norms based on appropriateness contains norms about fitting ways to ask for and reveal information in a particular situation (Nissenbaum 2004a, 119). These norms are about the *revelation* of information. The explicitness, rigidity and completeness of the set of norms applicable to a context vary (Nissenbaum 2004a, 124). For some contexts, the norms are vague and leave room for interpretation or complementation, while in other contexts they are distinct, elaborated and strict. For example, during an interview for a position as a waitress in an ordinary city centre restaurant, the interviewer is bound by strict norms of appropriateness that are codified in the rule of law. The purpose of an interview is finding a suitable candidate. In this context, requesting information about intimate details would be considered impertinent, as it would not be constructive for its purpose. In contrast with friendships, to which, according to Nissenbaum, few norms of appropriateness apply. In these relationships, it is pertinent to share and ask about a lot of different aspects of one's personal life (Nissenbaum 2004a).

2) According to Nissenbaum (2004a), there is another set of norms that complements the first set: norms of distribution. The norms address the *distribution* of information. Also, the set of distributional norms is determined by the context. The norms applicable can be complex and strict, which is the case for patient health information in which medical staff is bound by regulations that limit the distribution of information to others (Nissenbaum 2004a). In other cases the norms have considerable latitude, for example, when recommending the name of a person for a position in a company. Both sets of norms can differ. For example, it may be fitting between friends to exchange information about many aspects of their personal life – few norms of appropriateness apply – but the distribution of this information to other parties is subject to strict norms as confidentiality is often valued between friends.

According to Nissenbaum (2004a, 2004b and 2011) and Tavani and Moor (2001), these norms originate from social, political, and moral values.[40] Basing norms *solely* on the

---

[40] This might leave Nissenbaum's account open to the attack that the right to privacy can better be defended by referring to other principles. This critique is most forcefully advanced by Thomson (1975). Following Scanlon (1975), I will hold that one's interest in privacy cannot be captured by property rights or the right to bodily integrity. The fact that one may observe an object of mine does not need to be a violation of ownership but can be a violation of privacy. According to Scanlon: "ownership is relevant in determining the boundaries of our zone of privacy, but its relevance is determined by norms whose basis lies in our interest in privacy, not in the notion of ownership" (Scanlon, 1975, 318).

value and purposes *in practice* attached to a context would lead to consequences inconsistent with commonly held moral intuitions regarding privacy. Sometimes the failure to comply with moral principles and values can lead to people not getting the protection they deserve. Suppose that instead of considering it inappropriate, asking interviewees questions about intimate details of their private life, even if these details are irrelevant to the vacant position, is generally considered appropriate. In accordance with the prevailing social norms, the interviewee's claim to privacy would not extend to these details in this context; but based on fairness and equality, she should be warranted some protection in order to prevent discrimination and promote equal opportunities. There is a second, related counterintuitive consequence of relying on the *status quo*. Violating privacy can be rewarding; if systematic abuse becomes accepted as the norm, privacy can be reduced severely and undesirably. At other times, privacy can be inflated to include matters that do not deserve protection. For example, people may consider the financial investments of prominent political figures a context that merits non-disclosure. However, allowing them to secretly invest could conflict with their duties as representatives, and would obstruct, amongst others, the checks and balances needed for good governance; therefore extending privacy to financial investments by politicians or other prominent political figures would be undesirable.

Sometimes the norms applicable to a context are unclear, which is arguably the case with lifelogs as they constitute a novel context. Remember that a 'context' and 'situation' are general terms potentially applicable to many different things; a particular friendship can be a context, but searching for information on the Internet and using a lifelog are contexts as well.[41] In case digital technologies constitute or create new contexts in which the norms are unclear, Nissenbaum (2011, 44) suggests either to adopt the norms applicable to existing contexts that are similar in action or purpose, or, when there are no precedents, to assess the purposes and values of technology or procedure and how the access and distribution of information could affect these.

However, there seems no technology from which one can integrally adopt their sets of norms. No technology yet has the same abilities to offer users personal information about their past. The magnitude of information created by lifelog technology and the configuration of its parts make it distinctive from any other technology. Moreover, similar concepts that

---

[41] The context examined in this dissertation is further specified by offering a scenario and by specific goals, data, and devices for lifelogs. Lifelogging for other purposes such as those that might be applied by persons with dementia might require different considerations.

also have yet to be further developed, such as the Internet of Things and the Quantified-Self, are also recent inventions of which the values and purposes and the sets of norms to sustain privacy are arguably still unclear, and need to be further developed as well.

Therefore, for lifelog technology in this context, one needs to create novel sets of norms. According to Nissenbaum, an assessment of the norms begins by determining the values and principles promoted by the technology (Nissenbaum 2011, 44-45), and consider if the distribution or revelation of information would be warranted considering these values and purposes. Such an assessment would be similar to this: a particular lifelog technology is intended to significant support the lifelogger in improving his health - a worthwhile goal. This goal warrants the creation and distribution of information necessary for this purpose. However, the same information is also valuable for an insurance company that wants to use this information to unfavourably quote future customers or deny them altogether. The lifelog company which aims to maximise profits is tempted to sell the information. This commercial exchange does not seem to suit the purposes for which the information was created, because people might refrain from using lifelogs if they fear that their information is being purchased by insurers (and thereby they will fail to reap the benefits for health) or they might be denied affordable healthcare after the sale (and their health situation might be worse).[42] In addition, one can question if the selling of information is just or that it might unfairly disadvantage some lifeloggers. Consequently, a sale to an insurer seems to violate the values and principles promoted by lifelogs and other moral values and principles. As a result, the sale would be a violation of privacy. Instead of identifying the norms applicable to lifelog technology – which would be unattainable because of the multitude of lifelog devices and applications and the complexity of daily life -, in this chapter the ability of lifelog technology to conform to norms is discussed.

4.1.5 Control and privacy

Control over personal information is an aspect of privacy, although privacy is not defined by control. According to Tavani and Moor, it is the situation rather than the piece of information that determines which norms are in place to protect privacy (Tavani & Moor 2001; Tavani

---

[42] One could claim that for the lifelog company the purpose of this information was to maximise profits. The agreement between the customer and the company might be that the lifelogger allows the company to maximise profits, and the company supports the lifelogger with improving his or her health. Nonetheless, even in this case it seems doubtful that there are no norms in place that limit the selling of data that could be used to deny people affordable healthcare, especially since the use of lifelogs would actually hinder the purposes they were intended to serve.

2007, 12). Nissenbaum uses a similar interpretation in which contexts define norms regulating access to and distribution of personal information (Nissenbaum 2004a and 2011). After all, one piece of information is appropriate to be revealed or distributed in one context while inappropriate in another. The norms applicable in a 'situation' or 'context' that regulate intrusion, interference, and information access by others create a 'zone of privacy' (Moor 1997, 30). These zones of privacy allow people to control their privacy. For example, potential future employees and the interviewer in general have an idea of what information they are allowed to hide, and what information they are expected to reveal during an interview. The norms in place define how far the protection of privacy extends so that people know the control they can exercise over their personal information.

Tavani and Moor propose instruments to offer persons control over their personal information. This control does not have to be absolute, as is the case with control-based accounts of privacy (Tavani 2007). It requires that individuals have the ability to exert some influence over the disclosure and circulation of personal information. Tavani and Moor recommend three tools that the individual might use to exert control: choice, consent, and correction (2001, 8).

Choice entails the ability to choose privacy, which depends on being aware of how information is circulated and to what extent personal information is protected (Tavani & Moor 2001, 8). This exercise of control extends beyond normatively private situations and also includes naturally private situations. For example, if I want to do my grocery shopping without meeting acquaintances, I can choose to go to a shop in an area where I think I will have a small chance of bumping into them. I can do so, because I have a reasonable expectation that most people will have no source of information to trace my shopping except for them glancing directly into my basket. This way, I can choose privacy to some extent, which I could not do if information about my shopping behaviour was digitised and shared without my knowledge.

Consent to waive one's right to privacy is basically short for informed consent. For example, often one's house is a normatively private situation for strangers, but people can grant strangers access to it. In order to give consent, one needs to be provided with sufficient information to decide if one desires to waive one's normative claim to privacy in a specific situation when one has a right to do so. Similar to informed consent, it requires being free from coercion and some understanding about what one has agreed upon.

Correction allows people the opportunity to change erroneous information. Individuals should be able to access and revise data about themselves in order to prevent the spread and preservation of erroneous information.

These three instruments alone are insufficient to ensure that people have a satisfactory degree of control over their personal information. Foremost, the absence of structural protection of privacy would mean that citizens would have to make decisions, in every case encountering people wanting to access or distribute information. Current technology has vastly expanded the ability to create and distribute personal information. The sheer number of choices regarding their privacy that would need to be made would overwhelm an ordinary citizen when these decisions need to be made on a case by case basis. In order to allow a satisfactory degree of control, an environment needs to be created in which privacy is protected through other means than choice alone. Amongst others, robust national and international regulation to protect privacy is required.[43]

4.1.6 *Justification for the use of the principle*

As discussed before, respect for privacy is a *prima facie* principle. Therefore, a violation of this principle is a factor worthy of consideration, regardless of any other considerations in favour of this infringement. In a hypothetical situation where a benign dictator, who continuously infringes the privacy of her citizens, uses, and will only use, information obtained from these infringements to, successfully, benefit them, a situation is preferred in which the people would receive the very same benefits without the violation of privacy. The violation of privacy is a *prima facie* consideration against the acts of the dictator. Respect for privacy is a relatively novel principle within the ethical discourse, but it is most certainly no fringe principle. Following various scholars, it will be assumed that all known societies hold some norms, which set limits to information flows (Moore 1984; Tavani & Moor 2001;

---

[43] In order to protect privacy, Moor (1997) recommends three principles for policy: (1) "the Publicity Principle" (1997, 32), (2) "the Justification of Exceptions Principle" (1997, 32), and (3) "the Adjustment Principle" (1997, 32). The first one states that "rules and conditions governing private situations should be clear and known to the persons affected by them" (Moor 1997, 32). The second states that "a breach of a private situation is justified if and only if there is a great likelihood that the harm caused by the disclosure will be so much less than the harm prevented that an impartial person would permit breach of this and in morally similar situations" (Moor 1997, 32). The third states that "if special circumstances justify a change in the parameters of a private situation, then the alteration should become an explicit and public part of the rules and conditions governing the private situation" (Moor 1997, 32).The first and third are to inform people about the conditions and regulations in place relevant to their privacy and changes to these. The second one is a condition of proportionality stating that privacy considerations can be overridden when other considerations are judged decisive. Put into the terminology of this dissertation, there might be other *prima facie* principles, which outweigh privacy.

Tavani 2004; Nissenbaum 2004a), and that privacy is therefore part of the common morality as described by Beauchamp and Childress (2009).

Thus respect for privacy is always a *prima facie* consideration against actions that violate privacy. In addition, privacy can be regarded as instrumentally valuable, i.e. privacy is also valued on the basis of what one can achieve with it. The values protected by privacy can be manifold. The importance of privacy is often related to its instrumental value to personal freedom. People may act differently when they are scrutinised by others from how they would act without being watched. In addition, personal information or access to a person could be used to force that person to behave in a particular way. Surely it becomes more difficult to enforce particular behaviour if one lacks access to the person and/or information about him. Tavani and Moor are scholars that justify privacy, partly because it allows people the personal freedom to control their lives, and protect them from the influence of others (Tavani & Moor 2001; Tavani 2007).[44] Variants of the idea that privacy protects against the judgements of others, and thereby provides some level of autonomy have frequently been advanced (Allen 1999-2000; Gavison 1980, 423; Lessig 1999; Nissenbaum 1998, 2004a and b). Arguably, one can find early accounts that stress the importance of privacy (in which the term 'privacy' is not used) in the works of both Locke (1689) and Mill (1859), as they argue for a private sphere in which the state (and other third parties) cannot interfere. As the list in footnote 45 shows, there are many other values that are said to be affected by a failure to respect privacy.[45]

---

[44] Moor first attached intrinsic value to privacy (1990) but seems to have altered his defence of privacy slightly by accentuating its instrumental worth in more recent sources (Tavani & Moor 2001). Nonetheless principles can both be instrumentally and inherently valuable.

[45] Allen (2012) lists the following values and ends of privacy:
   1. "Self-expression: Opportunities for privacy allow individuals to better express their true personalities and values.
   2. Good Reputation: Privacy helps preserve reputations.
   3. Repose: Privacy may enable tranquility and relaxation.
   4. Intellectual Life: Privacy may enhance creativity and reflection, which may be good for an individual's own sake, but which can lead to useful cultural products and inventions.
   5. Intimacy and Formality: Opportunities for privacy are thought to enable individuals to keep some people at a distance, so that they can enjoy intense intimate relationships with others.
   6. Preferences and Traditions: Privacy allows the individual or groups of like-minded individuals the ability to plan undertakings and live in accord with preferences and traditions.
   7. Civility: Privacy norms sustain civility by condemning behaviors that offend courtesy, honor, and appropriateness.
   8. Human Dignity: Philosophers have said that respect for privacy is, in many ways, respect for human dignity itself.

4.2　Challenges to privacy

The effect of the technology on privacy is discussed by detailing the way lifelogs could influence the distribution and disclosure of personal information and lifeloggers' and non-lifeloggers' control over their privacy. This part is descriptive as it explains the potential effect of lifelogs on privacy.

The effect of lifelog technology on privacy will be explained in five parts. (1) The properties of lifelog technology that underlie most of the concerns for privacy are explained first. (2) Following that the ways in which lifelogs can infringe the privacy of other people than lifeloggers are discussed second. (3) Next, the ways in which lifelogs can infringe the privacy of primarily the lifelogger are examined. (4) In the fourth part, an advantage of lifelog technology for privacy is mentioned. (5) In the last part, factors are explained that mitigate the issues with privacy identified.

4.2.1　Effects on personal information

Two tendencies, (1) the increase in personal information, and (2) the facilitation of the distribution, and revelation of personal information, which underline most of the issues concerning privacy, will be discussed. A basic understanding of these tendencies will prove invaluable for understanding the effects on privacy caused by lifelog technology.

4.2.1.1　Increase in personal information

One of the reasons as to why lifelogs generate idiosyncratic challenges is the manner in which they gather data, which can lead to unprecedented amounts of personal information being available digitally. There are five ways in which lifelogs can increase personal information:

1) Lifelogging devices lessen the effort needed to create personal data about oneself or others. Unlike many other devices capturing similar kinds of data, lifelog devices and applications capture this information automatically, such as the Vicon Revue or the Narrative Clip. The pictures they can take, which can reach a staggering number of 3000 a day, exist for the sole purpose of lifelogging. For instance, taking a photo using a smartphone requires a

---

9. Limited Government: Privacy rights against government demand that state power is limited and unobtrusive, as liberal democracy requires.
10. Toleration: Privacy rights demand that government tolerate differences among individuals and groups.
11. Autonomy: An aspect of liberty, privacy fosters the development and exercise of autonomy.
12. Individualism: Privacy fosters individualism, and it is not fairly condemned as a purely individualistic value at odds with ideals of a cooperative, efficient democratic community" (Allen 2012, 5-6).

set of actions that can be avoided when using lifelogging devices: typically when using the camera on a smartphone, one first has to locate one's phone, position it in one's hands, unlock it, activate the camera, point the camera and then one can press a button to snap the picture. Cameras such as Narrative Clip or the Vicon Revue only require activation and deployment once, and after that they capture data autonomously.

2) Some data sources are created solely for the purposes of lifelogging. This is most evident with devices that are developed exclusively for this, such as the aforementioned Vicon Revue and Narrative Clip. In addition, data can also be harvested from sources that are already currently available, and sometimes firmly embedded into society, but which are not initially designed to provide the user with information about their past. These data sources were originally designed and primarily used for other purposes than lifelogging, and their usefulness to lifelogs is only a by-product. Data sources are suitable insofar as their data can convey information about the lifelogger or the environment in which he is situated when lifelogging. As more devices create digital data suitable for lifelogging, and more activities take place on the WWW leaving digital traces, more devices become suited to the purposes of lifelogging. Indeed, in order to create lifelogs, existing devices might suffice and no additional data sources may need to be developed.[46] Yet some existing data sources are not yet exploited to convey personal information about an individual. For instance, energy consumption in the home reveals significant information about someone's lifestyle, but is not used for these purposes.[47] To transform a device into a lifelogging device, some devices will require modification. For different reasons, the smartphone is a likely candidate to become a lifelogging device (this is more extensively explained in *2.3.1 Brief history and current state of lifelogs*). Transforming a smartphone into a lifelogging device can be as simple as installing an application. Already lifelog applications are available for the smartphone.

3) Lifelogs can create novel information from existing data by processing data, e.g. augmenting data with semantic meaning to improve information retrieval. For instance, if one captures photos in an archive, but one cannot query the content of the photos, the archive

---

[46] For instance, for voice, location, image, movement and body signals a wide range of sensor devices is at hand, including dictaphones, smartphones, digital cameras, heart rate monitors, and other wearable devices that enable us to record these types of signals. Also digital or non-wearable devices can deliver information to lifelogs. Existing data such as search queries, e-mails, visited websites, financial transactions, and domestic energy meter readings can be equally useful as contributing to lifelogs.

[47] By processing data from energy meter readings one can discover living patterns, e.g. the times and frequencies a person prepares her food, wakes up, or uses the electric shower.

would be of little use as an automated biography as it would become too burdensome to retrieve relevant information. Suppose one is looking to retrieve the name and location of a restaurant in which one had lunch with an acquaintance a couple of months ago. Sifting through a collection of photos would be time consuming and impractical. Allowing search queries, such as using terms from human language, e.g. 'lunch' or 'Dublin 1', demands the augmentation of lifelog data with semantic meaning. Instead of having only a photo, one would need tools to dissect information from the photo. Instead of just collecting and storing data, developers need to quantify and qualify data to improve information retrieval, so that the lifelog becomes more useful to the average lifelogger. In doing so, lifelogs can increase the amount of personal information digitally available, even when lifelogs would only use existing data.

4) The processing of data from different data sources taken together allows for the creation of more information than one could have obtained from individual data sources processed separately.[48] By collecting data from different sources, such as adding GPS coordinates and recorded Bluetooth signals to photo images, lifelogs can offer more exact information about a person than these data sources could reveal separately (Byrne et al. 2007). The collection of data by lifelogs provides unprecedented possibilities for gathering a depth and variety of (personal) information untenable when using the data sources separately. Again, even when lifelogs only collect data that exist irrespectively of lifelog technology, the fact that lifelog technology brings together several sources of data makes it possible to retrieve more information than when processing data sources separately.

5) The lifelog technology most likely requires duplicates of existing data. Unless the lifelog only uses devices especially created for the lifelog, such as wearable cameras, to create the lifelog, data from several sources need to be copied and transferred to the lifelog. For example, instead of having data from smart energy meters on the internal storage of the meter or in a cloud from the company offering smart meters, these data are also stored within the lifelog. As a result, a larger quantity of personal data is available digitally.

---

[48] Capturing can improve by combining sources of data. Some lifelogging devices can react to their environment when combining sources of information. The Vicon Revue combines the data from an accelerometer, a magnetometer, an infrared motion detector, a light colour and intensity sensor, a temperature sensor and a 3 megapixel sensor. This information can be found at: http://viconrevue.com/product.html. By using sensors which sense different conditions of the physical world, they can detect new situations of potential interest as a cue to start taking photos.

Conclusion: Lifelogs can increase the amount of personal information in at least five different ways: (1) they lessen the effort needed to gather data; (2) they can be a reason to transform devices with the purpose of creating personal information or develop novel devices; (3) lifelogs create novel personal information to improve information retrieval; (4) the bundling of data sources enhances the ability to create personal information; (5) lifelogs could require duplicates of existing information.

4.2.1.2 Facilitating the revelation and distribution of data

The digitising of personal information can have far-reaching consequences relevant to privacy as it determines both what information can be disclosed as well as distributed. Five ways are presented in which lifelogs influence the flow of information.

1) First of all, the centralisation of information facilitates the retrieval in the sense that it is accessible without having to go through different platforms. A well-functioning lifelog gathers and organises data in a way one can retrieve the information about aspects of one's past without much effort. Digital storage can lessen the effort necessary to retrieve information: for instance, there is no need to visit one's parent's house to retrieve some photo albums. Even in the digital realm, in which one may have to use different platforms to access data, e.g. web-based email services, social networking sites, e-banking websites, online medical records, lifelogs facilitate access to personal information, as one only has to access a single platform, the lifelog, that contains all this information. The concentration of information lessens the resources and time required for retrieval.

2) The second consequence of lifelogging is that temporal limitations to distribution of personal information are alleviated in several ways. Unlike analogue archives in the possession of governmental agencies or public institutions, lifelogs have no closing times. Especially when lifelogs are stored on clouds, i.e. available through a network most typically the Internet, they become accessible at any moment from anywhere with a decent Internet connection. Temporal limitations are also alleviated with regard to the gathering of data. Sensors function around the clock, and there are sensing devices that can capture data at any time of the day. Finally, and maybe most importantly, unlike analogue sources such as print, digital data does not decay. Compared with previous information technologies, such as hard copy print, the duration of ordinary digital information is extended drastically (Mayer-Schönberger 2009). Mayer-Schönberger (2009, 56) mentions that digital data can be stored on any device with sufficient and accessible digital storage, and shared without any loss of

quality in contrast to analogue copies that often suffer from huge losses of information when being duplicated.[49]

3) The third point here is that spatial limitations to distribution are being alleviated. By using servers connected to the Internet, personal information can be accessed from anywhere and distributed to anywhere. Internet connections most likely will only further proliferate in the foreseeable future. In addition, devices equipped with sensors are becoming increasingly portable, sophisticated and connected. As a result, one can obtain data in remote areas or under unfavourable conditions. So information can be created virtually anywhere as well as accessed from and distributed to anywhere. Moreover, the storage of this information requires less physical storage space than is needed when storing hard copy paper files. There may barely even be a need to physically possess personal storage space because cloud storage allows the storage of the main body of information on distant servers.

4) Fourthly, data gathering devices have become more ubiquitous. An increasing amount of portable devices (such as smartphones and other wearable devices) as well as devices embedded in the environment (such as ambient intelligent devices) are becoming suitable for lifelogging. This means that a growing number of devices produce information that can reveal some information about the lifelogger or others in his or her environment. Moreover, more activities are carried out online, producing a trail of data that is suitable for lifelogs. It becomes increasingly difficult to find aspects of life that are or can be completely guarded from being captured digitally.

5) Finally, also networking technology has become more pervasive. Lower prices for storage, processors, and Internet connections, will facilitate the use of lifelogs and increase the availability of digital information. The devices needed to create or access lifelogs will

---

[49] There are, however, a few remarks to be made which might prove important to the durability. File formats change so a format can become outdated while the ability to read or convert it might not be available. The piece of data would be identical to what it was but ultimately becomes useless. Moreover, even though hard drives might last for years they will fail at some point in time. If storage space is damaged and there are no back-ups available, then data is lost. Although more digital information seems to be stored for longer when it is digitised, in extraordinary situations analogue data has been conserved for centuries and millennia. For example, a Madonna painted on canvas has been dated back to the 13th century (Time Magazine 1955) and the Etruscans left behind a book that is dated back to 600 BC (BBC 2003). It is questionable if digital information would be preserved for this amount of time. The infrastructure and knowhow to read and recognise a hard drive as something that stores information might disappear in time. Someone who finds the remains of a computer in the distant future might not recognise it as such. A book or a painting has remained recognisable as such for millennia. Even though we are unable to read the Etruscan book, we are aware that it is a book storing some kind of information. Hence, although more information might last longer during, data might remain less durable than some exceptional pieces of analogue information.

become increasingly available. After all, lifelogs can be created by only using the Internet and a smartphone. Increased access to these things facilitates the creation, spread, and duplication of lifelog information.

Conclusion: These five tendencies allow one to lifelog at anytime and anywhere and to access and share information from anywhere at any time with little burden to either the sharer or the person accessing this information. Moreover, it facilitates the creation of duplicates. Indeed, because of these tendencies digital data can proliferate.

4.2.2 Challenges to the privacy of others

Lifelog technology could reduce the privacy of people other than the lifelogger. Reductions of privacy caused by active lifeloggers to others have a distinctive weight. The lifelogger could have decided autonomously that, despite the negative consequences of using lifelogs, recording his information was in his best interests. A non-lifelogger may not have chosen to have his privacy reduced (or may not have had a choice at all) and, therefore, reductions of his privacy are unlikely to be the result of an autonomous decision by him. If the choice to lifelog and reduce one's privacy is the result of an autonomous choice, then respect for autonomy can become a *prima facie* principle in favour of lifelogging. In case the reduction or violation of privacy was not the result of an autonomous choice, the principle of respect for autonomy can become a *prima facie* principle against lifelogging.[50] The following parts discuss issues predominantly but not exclusively associated with the privacy of people being recorded by the lifelogger.

4.2.2.1 **Reduced control over personal information**

Information about others can become part of lifelogs, because one seldom lives in complete solitude. Therefore, a comprehensive biography of one's life would contain information about the people one shares one's life with.

The most blatant example of devices capturing information about others is the use of a wearable camera, as it is directed outwards, towards the lifelogger's environment rather than aimed at the lifelogger. The lifelogger's own image is only captured incidentally through reflections. Information about the lifelogger is derived primarily from the environment in which one is located. As a result, any passer-by can be captured. These people can be unfamiliar with or unaware of the lifelogger, which evidently impairs their choice to be

---

[50] This is also a reason why the conditions under which one becomes a lifelogger are relevant.

lifelogged. As a result, these people are likely to lack the opportunity to curate or correct personal information captured about them. Moreover, lifelog data from a lifelogger might be copied and distributed allowing little opportunity for control such as correction, choice or consent.

In theory, it seems possible to avoid creating information about others within the lifelog by designing the lifelog carefully. Lifelogs that capture and store no personal information about others avoid harming the privacy of others. In practice, it seems unlikely that lifelogs are rid of information that can be attributed to others. Three reasons for this will be provided below.

1) The past and current state of lifelogging, e.g. MyLifeBits, the SenseCam, Narrative Clip and Autographer, includes devices that capture imagery of the environment rather than the lifelogger. The websites of the Narrative Clip and the Autographer advertise their product by promoting their ability to capture information about loved ones. Indeed, from the outset lifelogging was about comprehensiveness, and most certainly included information about others the lifelogger was in contact with. Microsoft described MyLifeBits as "a lifetime store of everything" (Microsoft 2014). The DARPA lifelog project aimed "to trace the "threads" of an individual's life in terms of events, states, and relationships" (DARPA/IPTO 2003).

2) Excluding information about others would lead to a great loss of functionality. For example, sousveillance depends on the lifelogger's ability to capture information about others, specifically people with authority. Also, excluding all information about others is less straightforward to achieve than one might initially expect as it would require the avoidance of any data that potentially can be attributed or can refer to others; data such as Bluetooth, photos, videos, wireless connections, e-mails, text messages, GPS, calendars, or metadata about phone calls could reveal information that indirectly or directly can be attributed to other people. Even without recording others directly, lifelogs might reveal information about others. Recording information about body signs, GPS, *et cetera* can reveal a great deal about the lifelogger's interactions with their environment and, as a result, others that may be in their presence, e.g. information that the lifelogger was spending much time in someone's house will likely reveal a close relationship with that person.

3) Governmental agencies and corporations might be able to cross-reference data from different lifelogs and by doing so gain novel information. In this case, the lifelog does not have to capture information about others to reveal information about them. This information

is difficult to obtain for an individual, as he would need to gain access to multiple lifelogs and process their data, but sufficiently funded governmental agencies might be able to do so. The US National Security Agency (NSA) is such a governmental agency with an astonishing budget which was around $11 billion in 2013 (Gellman & Miller 2013). By tracking cellular phone locations worldwide, the NSA can track individuals and their relationships (Gellman & Soltani 2013; Kravets 2013). Citizens ordinarily would not have the technological know-how, equipment, or access to data to do so.

Conclusion: It is very likely that lifelogging devices will affect the privacy of others. The evident solution to minimise information about others is to develop lifelogs that do not contain data that can be attributed to others or design a lifelog in such a manner that information about others cannot be retrieved.[51] However, the history and current state of lifelogging show an interest in using devices that predominantly capture information about others and only indirectly capture information about the lifelogger himself. Moreover, many data sources can be used to retrieve information about others. More importantly, excluding information about others could cause major reductions of functionality. Finally powerful organisation could gain access to multiple lifelogs, and obtain information by cross-referencing and triangulating data that does not directly refer to or can be attributed to others.

4.2.2.2 Distinguishing normatively private situations

The issues that lifelogs cause with regard to the privacy of others could be even more pernicious, as even the benevolent lifelogger who is aware of the prevailing privacy norms can still fail to protect the privacy of others. Strategies that rely on the discretion of the lifelogger to decide whether to record an event will often lead to unsatisfactory outcomes. The assumption that one has sufficient understanding about the situation one intends to lifelog is not always justified. The characteristics that define a context are sometimes fuzzy and/or unknown to the person recording, or to the people whose information has been stored.[52]

1) The lifelogger and the person being recorded can lack full information about a situation. In the most ordinary way, unfamiliarity with the environment can make one infringe someone else's privacy. This can happen by accident, for example by opening a door that should have been left unopened. When using devices that capture information

---

[51] Even when one decides to use images from a camera, the lifelog can be made to select photos with people blurred or without people on it. This way some of the functionality of a camera might be preserved.
[52] The issues will be discussed in more detail in section *4.2.2.4 Concerns caused by the longevity of information.*

autonomously such dull mistakes can result in situations being captured and digitised inappropriately. As a result, there may be consequences to making these ordinary mistakes which were not there before the advent of lifelogging technology. Also, situations can change abruptly. People sometimes profess intimate details when one least expects them to. More subtle is unfamiliarity with the prevailing norms. People may be unaware that the norms prescribe that one ought to refrain from capturing information or, conversely, that it is appropriate for them to be recorded. In addition, the lifelogger, as well as the other persons who are captured, cannot choose what is to be revealed because they may fail to understand what information can be gathered or is gathered. In this case it is unfamiliarity with technology that causes the problem.

2) The fact that lifelogs capture information autonomously has drawbacks regarding control. One may be able to choose the devices to lifelog, and to some degree the data one gathers; however, the fact that lifelogs gather data autonomously entails that some of the intentionality that is required when the collection of data is driven manually is lost; taking pictures of a scene manually when one has to grab and point the camera and press a button requires a more conscious effort than automatically capturing those pictures by attaching the camera to one's jacket and activating it when leaving the house. The latter is more likely to result in the accidental or unintended capturing of information.

3) Another issue of relevance here is that a lifelog might extract more information from a situation than one could obtain through experience. Identification software can now recognise emotions more precisely, GPS and Wi-Fi can track distances more accurately than a person can, and a heart rate monitor can measure heartbeats over an extensive period of time. This information can go beyond one's perception, let alone what one remembers. Furthermore, as the current trend of sensor devices becoming more responsive persists, they will be able to capture more detail.[53] When people take photos of their children playing a football match in a park they will also capture the environment in which they play. The higher the quality of the photo, the more the photo could reveal of the environment. The lifelog devices (combined) might *see* or *hear*, i.e. capture, more in particular conditions than the lifelogger could possibly perceive at that moment. This way, the photographer could accidentally capture a man quickly changing his clothes between half open curtains or the voices of a couple nearby whispering their disagreements thinking they are out of earshot.

---

[53] In addition, the development of sensors also appears to conform to Moore's Law –the observation that the number of transistors on an affordable chip would double every two years (Moore 1965).

An additional concern is that seemingly harmless information can reveal more than the person recorded might initially expected it to. The lifelog may extract information about a situation one may be unable to infer oneself with such probability. In addition to sensors, also algorithms seem to improve. Research shows that it is possible to predict the status of one's relationship based on data from a social networking site (Backstrom & Kleinberg 2014), that mental disorders can be revealed by eye-tracking software (Tseng et al. 2013), or that the risk of being physically assaulted is partly determined by one's walking style (Gunns, Johnston & Hudson 2002).[54] One may be unaware that this information can be gathered from seemingly innocuous sources of information, and thereby one's control over the revelation of this information is reduced. Indeed, even if one would be aware that this information can be obtained from lifelog technology, the person whose personal information has been recorded may not be able to conceal it.

Conclusion: Even benevolent lifeloggers can fail to respect the privacy of others, and people aware of privacy issues can encounter unexpected issues. Normatively private situations are not clearly demarcated as such. In addition, lifeloggers may capture more than they intended to. These issues are largely solved by avoiding the capturing of information about others. A way to reduce these issues would be to decrease the sensitivity of sensor devices, and limit the information retrieval, so that information about others is minimised, e.g. by developing cameras or microphones that capture only the close environment instead of using high-end sensors, and by limiting the application of recognition software.

4.2.2.3   Reduced expectation of privacy

A widespread proliferation of devices which can capture information about others could reduce people's expectation of privacy. Issues with control are exacerbated by the fact that lifelog devices can be unrecognisable as such, or perhaps are camouflaged or hidden.

1) Lifelogging devices can be small: for example, Narrative Clip, the lifelogging device from Memoto, is the size of a postage stamp, making it difficult for others to notice when it is being used.[55] Moreover, some devices do not necessarily appear to others to be lifelogging devices, or do not show when they are active as such. For example, there is no

---

[54] Even mental states such as mental illnesses or undesirable character traits, such as narcissism and/or social anxiety, can be identified from posts on websites (Fernandez, Levinson & Rodebaugh 2012; Golbeck, Robles & Turner 2011; Mehdizadeh 2010).

[55] In some cases there are good reasons to hide sensor technology. For people with dementia sensor devices might be perceived as a source of stigma when visible (King et al. 2013).

perceptible difference between a smartphone that is lifelogging, and one that is idle when one lays it casually on the table during a conversation. Moreover, some lifelogging devices will become integrated into everyday life to such a degree that the user could not function without them. Take for example Google Glass, a device that is (at this stage visibly) integrated into one's spectacle frame. If Google develops these glasses with prescription lenses – which it has started doing (Bohn 2014) - people might have to use them for eyesight. In some instances, users will not be able to take them off, as they might not carry (around) an extra pair of glasses. These glasses do not necessarily indicate that they are recording. Even if the wearer is asked not to record, he could capture others without their consent or without them being able to check if they are recording: a higher level of insecurity about one's privacy can be created with those devices. These issues become more troublesome when lifelog devices deploy high-end sensors that may capture personal information from a greater distance than one would normally see or hear. In those cases one may be recorded without being able to certify oneself that one is not recorded.

Such issues become especially relevant with the advent of ambient intelligence and ubiquitous computing. In 1991, Mark Weiser published a well-known essay 'The computer for the 21st Century' in *Scientific American*, in which he predicted a third generation of computer systems (Weiser 1991). The first generation was only accessible to experts and consisted of large mainframe computers. The second generation democratised the use of computer systems, and made them accessible to a wide range of consumers, e.g. the tablets, smartphones, desktop and laptops computers currently used at home. According to Weiser (1991), this generation was merely transitional. His prediction was that the third stage would consist of computers which would be integrated into everyday life to such an extent that their use would go unnoticed. This has been coined 'ubiquitous computing' (Weiser 1991, 89). Ambient intelligent devices are likely to gather personal data and also be embedded into everyday life (Aarts & Marzano 2003).[56] When these devices are embedded into the environment in which they function, they may go unnoticed adding insecurity about whether or not one is being recorded.

---

[56] However, there are certain characteristics that are widely ascribed to ambient intelligence – a term that is still lacking a generally accepted definition:
- Embedded: integrated in the environment
- Context aware: ability to recognize individual users and situations
- Personalized: they can be made to conform to individual preferences
- Adaptive: they can change as a reaction
- Anticipatory: they can change without interference (Aarts & Marzano 2003, 14)

Conclusion: If the use of these devices for lifelogging becomes widespread, one would, at times, for prudential reasons, have to act as if one has no privacy, even if one may have a right to it and, indeed, even if the others are, in fact, respecting one's privacy as one would be unsure if this is the case. For this reason, even without *de facto* reducing privacy, a widespread use of lifelog devices can at times obscure one's control over privacy disallowing one to act as if one has privacy.

The weight of this issue might decrease over time as familiarity with the technology increases the chance that lifelog devices that remain perceptible are recognised as such. Similarly, people are now generally able to recognise most photo cameras as being photo cameras, and this allows them to anticipate their use. In addition, over time, the moral, legal, and social norms will develop that set of limitations on the use of lifelogging devices. The norms will allow one to assume some privacy in some situations.

One way to accommodate this issue is to prevent these devices from being camouflaged or hidden. Developing devices in such a way that it is immediately clear when they are active (e.g. the red light on a camera) and inactive (e.g. low tech solutions such as covering the lens of a wearable camera are highly desirable) informs people of the privacy they enjoy. In addition, prevention of the integration of high-end sensors enlarges the chance that one is not being recorded by people outside one's peripheral vision. Nonetheless, lifelog technology that captures audio or the imagery of others is expected to have a detrimental effect to the privacy one can reasonably expect.

4.2.2.4 Concerns caused by the longevity of information

The longevity of information could pose problems by itself. The storage of data could be appropriate at the time of capturing, while at a later stage it becomes inappropriate. This issue concerns personal information that, because of lifelog technology, comes under the control of others. Concerns with longevity of data are caused because lifeloggers capture information about other people than themselves, but they could also result from the access to and/or distribution of lifelog data by other parties than the lifelogger.

1) One of the issues with the longevity of information is that individuals change. In the scenario, Paula found images of a superior who was drunk at a party (*2.5 Scenario*). The impression invoked by these photos could ill-reflect his current lifestyle. His behaviour could have been incidental (and maybe accidental, not realising the percentage of alcohol contained in his drink), or he could have changed his life and lived in abstinence ever since. So the

information might be correct, but ultimately still provide an incorrect impression. Sending these photos to his superiors, or sharing these photos with colleagues might be inappropriate and unfair, while it might have been more acceptable if he was not their manager or just a complete stranger.

Previous behaviour might poorly reflect one's current attitude, and it might be unfair to hold this information against a person. In law, this has materialised by allowing bankruptcies and some convictions to be expunged from one's financial or criminal records. This is the 'clean slate' argument (Koops 2011). According to him, one can have a reasonable need to stop being reminded and start anew (Koops 2011). Also, for social relationships non-forgetting can be negative, as people would be constantly reminded of their mistakes and disagreements, even if reconciliation and alteration have taken place (Allen 2008; Murata 2011). As shown in the literature review (*3.2.1 Challenges*), various scholars have identified such issues in relation to lifelogs (Allen 2008; Bannon 2006; Bannon 2011; Byrne, Kelly & Jones 2010; Clowes 2012; Van Dijck 2012; Dodge & Kitchin 2007; Dodge 2007; Van Den Eede 2011; Koops 2011; Murata 2011; Nack 2005; Rawassizadeh 2011; Sonvilla-Weiss 2008).

2) Also the environment in which data obtains their significance and meaning can change. The environment in which one is situated is dynamic; individuals, communities and organisations in one's environment may change the things they consider blameworthy and/or praiseworthy.[57] Over time different kinds of behaviour can be penalised and rewarded. The concerns with retention were less problematic when spatial, temporal and distributional limitations were still more forcefully in place as it was easier to 'escape' one's past by moving or through forgetting. Sometimes the change in attitude towards something is felt dearly. Van den Hoven (2008) mentions the Nazi occupation of the Netherlands. The registration of personal information under the Dutch rule might have had little significance, but during the occupation the Nazis could effectively target Jews by accessing the Dutch administration (Van den Hoven 2008, 311). Being identified as a Jew became a threat to one's life.[58] The future usage of data is difficult, if not impossible to predict. By storing

---

[57] This proves especially troublesome if information about a person is accessed by other people than that person, such as the lifelogger about other people, corporations, government agencies, or other third parties sometimes with nefarious intentions.

[58] Van den Hoven does not consider this a violation of privacy but an information based harm. However, if the databases are considered part of an exchange between the Dutch authorities and its citizens, than the access by a third party would be a violation similar to a third party accessing correspondence between two people over e-

digital data indefinitely, and allowing the proliferation of them, one gambles that this information will not negatively affect one or other members of the community at large over time.

3) Finally, the technology itself can change. Another issue related to the longevity of data is that it is impossible to assess what information can be obtained from data over time. Novel information can be inferred from existing data by improving retrieval techniques, cross-correlating information and developing or adding new data sources to existing ones. The data of lifelogs could be used to discover new trends and correlations, for example between health and particular behaviour. Subsequently, data, previously considered harmless to privacy, could reveal undesirable information. One tendency of considerable interest regarding privacy and lifelogs are the improvements made to identify individuals by means of data.[59] Identification can be based on physical characteristics or behavioural patterns. Improved identification technology will lead to more data potentially being attributed to individuals.[60] The usage of bodily characteristics as identifiers is also important because one cannot change one's body, and to a certain extent one's behavioural patterns, so one's ability to distance oneself from this information, now or in the future, is impaired. Photography has had the functionality of identifying people from its early adaptation in Ireland in the 19th century. By capturing the image of prisoners, it became possible to recognise repeat offenders, a category that barely existed before.[61] Today, identification technology has long surpassed the manual identification of persons on photos. For example, Google's Picasa, an online photo storage and organising website in which people on photos can be 'tagged', identified and annotated, using facial recognition technology (Google 2013). If identification techniques are combined with the alleviation of distributional limitations, and the increase and comprehensiveness of personal information, it becomes clear that it will become

---

mail. The issue at play is that information within a specific context serves purposes and to use that information for a different context can be inappropriate.

[59] This tendency is spurred by the increase of memory speed and storing space, both of which can be accounted for using Moore's Law and improvements in identification techniques. The body alone can be tracked using different properties, such as the ear, odour, heartbeat, voice, the iris, the periocular region, fingerprints, sweat, face recognition, DNA, and gait (Shachtman & Beckhusen 2013).

[60] Currently there are various projects and start-ups running with different motives that make an effort to improve facial recognition. An example is Cara, a company which aspires to bring facial recognition technology to individuals on their mobile phones. They aim to provide facial recognition for people within a range of less than 8 meters. More information can be found at: https://imrsv.com/developers.

[61] Information about this can be found at the museum of Kilmainham Gaol, Dublin, Republic of Ireland.

increasingly hard to distance one from one's past or escape being monitored. Neither moving away nor time would rid oneself of previously gathered data.[62]

Conclusion: The possibility that the lifelogger, his environment or the technology changes, and, consequently, the data stored obtain unforeseen meaning or significance is present. One cannot protect oneself by adjusting one's behaviour as one will be unable to predict the exact changes in the environment. There seems to be no evident technological solution to protect the person recorded against data that can be stored for an indefinite amount of time, besides ensuring that lifelogs contain information that only refers to the lifelogger and that this information is not spread to or accessed by others.

There have been attempts to find a technological solution to this issue. Dodge and Kitchin (2005; 2007) proposed to incorporate a technological variation of biological forgetting within the design of lifelogs. Their account of forgetting, which is based on the imperfections of memory as identified by Schacter (2001), is not solely the omission of information but also imitates remembering incorrectly. Their built-in mechanism for technological forgetting is materialised through techniques such as temporarily blocking information retrieval, changing details over time, and imperfectly recording data while leaving the broader picture intact (Dodge & Kitchin 2005). They assert that by developing software that preserves the main storylines while randomly forgetting more specific information, one would still possess more information due to the lifelog than one would have had without the technology. The result of incorporating forgetting into the fabric of a lifelog is that the lifelogger could not be confident that the retrieved information is true or that elements were left out; forgetting renders information less reliable. This would reduce issues with surveillance and enhance one's control over the past (Dodge & Kitchin 2007, 18). However, some researchers (O'Hara, Tuffield & Shadbolt 2009; O'Hara 2012) argue that forgetting is contrary to the *raison d'être* of lifelogs and that by building in forgetting, developers would be throwing out the baby with the bath water, which seems correct as it undermines the main purpose for which lifelog technology is developed.[63]

---

[62] The Irishman Larry Murphy who is a convicted rapist but also widely suspected of being a serial killer is 'chased' by the media and citizens who are trying to uncover his whereabouts (Williams 2013). There is even a Facebook page with nearly 11.000 followers (10-12-2013): https://www.facebook.com/pages/Larry-Murphy-Sightings-Tracker. The home addresses of celebrities seem relatively easy to find. By capturing and sharing information automatically, the net would be casted even wider.
[63] Large parts of this paragraph can be found in Jacquemard et al. 2014.

4.2.3 Challenges to privacy of the lifelogger

Even when lifelogs only obtain information that refers to the lifelogger or that can only be attributed to the lifelogger, which would be a sparse lifelog, the fact that the information is stored and made digitally retrievable could jeopardise their privacy.

4.2.3.1 Concerns regarding control over the creation of data

It is reasonable to assume that the lifelogger will have some control over what data are created and stored when using lifelog devices and applications. The lifelogger's control over the creation of data has implications for the information that can be revealed and distributed from lifelogs. Some control by the lifelogger over the lifelog technology is assumed because most people would prefer to keep some aspects of their lives or other people's lives unrecorded. Without control, this would be impossible, and the lifelog technology would most likely fail to attract a large following. Lifelog devices can create data whilst the lifelogger may have little understanding of what data they create and store, and for what purposes. However, the level of lifeloggers' control over the functioning of the device can be unsatisfactory. There are six issues with transparency about the data created identified.

1) The outside of a lifelog device or its graphic user interface (GUI) will reveal little of its internal functioning. Lifelog companies could easily hide processes from ordinary lifeloggers. Often the lifelogger will depend on the discretion of the lifelog company to be informed of the data created and potentially distributed to other parties. This has caused controversy, for instance, when Apple logged data from the iPhone that could be used to determine the location of its consumers (Bilton 2011). They did so, even when location services were disabled by the user, providing them with a false idea of control. Furthermore, even when there are mechanisms in place to control the creation and storage of data, one could be unaware of them, such as settings to protect privacy, or they might be too complex for ordinary users. This has prompted the World Wide Web Consortium (W3C) to recommend that privacy preferences should be formulated in a language understandable to its end users (W3C 2006).

2) Offering people instruments for control can require compromises and time and resources that a company might not be willing to spend. The threshold for a company to enter the market of lifelog applications can be low, allowing people with little expertise or funding to enter the market. For one, there might be little start-up capital needed to develop a lifelog product. Businesses might gain their starting capital through bootstrapping, i.e. funding the

development of the technologies with their own means. As a consequence, one can start a company without having sufficient funding to adjust the applications to ethical demands. After all, things such as security and expertise can be expensive. In addition, the market for applications and devices is competitive, allowing little time for developers to carefully build a reputation or test its products. Many developers may feel the need to fix a product after it has been released. This attitude is formidably embodied in Facebook's former mantra "move fast and break things", as written in Zuckerberg's letter to potential investors before Facebook's initial public offering in February 2012.[64] He offered the following motivation in the same letter: "if you never break anything, you're probably not moving fast enough". Especially when the corporation is small and unknown, it may suffer little from the backlash of violating consumer trust as it has no name to lose. Meanwhile, these small companies could handle highly sensitive personal content.

Furthermore, increasing control over a device might require adding functionalities that can compromise the user-friendliness or the attractiveness of the appearance of the device. Additional buttons can compromise aesthetics, as it may make the user-interface or the appearance of the device less appealing. When considering 'stylish' wearable devices such as the Misfit Shine or the Narrative Clip, those devices distinguish themselves by their minimalism, lacking buttons or a display. In addition, a device or application that has additional buttons and settings can become more complicated to use. Extending control while maintaining user-friendliness and aesthetical appeal can be burdensome.

3) Another complicating factor is a multitude of parties might be involved in lifelogging. A browsing session on the WWW brings one into contact with a stupendous amount of other parties that can create information about one's visit (without requiring consent or offering one a choice). Third parties could be introduced to the lifelog by allowing applications or devices to be added to the lifelog to increase functionality or by allowing advertisement companies to track people's behaviour in order to improve the effectivity of advertising. Currently, for these purposes third party applications are available for a diverse range of devices such as smartphones and desktop computers. Applications for smartphones can have low privacy standards, and some applications fail to provide the consumer with

---

[64] The letter can be found at http://www.wired.com/2012/02/zuck-letter/ [Accessed 13-05-2014]. Currently the company is at a stage in which reliability becomes essential for further growth especially as it aims to become a platform which other developers need to trust to develop their product. In this light Facebook's change of mantra from "move fast and break things" to "move fast with stable infrastructure" (Levy 2014) can be seen.

basic instruments to protect their privacy, such as privacy policies (Thurm & Kane 2010). The processing of personal data can be opaque and the companies behind those applications might lack the name or the reputation to suffer much from breaches of trust. Even in cases they ask for permission, these requests can be formulated so vaguely that users have virtually no idea of how their information is used (Kelley et al. 2012). Moreover, these companies can have a motive to infringe privacy, as the gathering and selling of personal information could be profitable, while informing the users about the information they generate could deter them from purchasing the device or application.

4) Consumers can provide incentives to weaken the security of technological devices. One of these incentives is the request for more functionality without necessarily requiring that these functionalities are ethically sound. Stacking the lifelog with all kinds of applications and devices that can find novel information, or add novel data sources could attract a far larger market than when lifelogs only offer a selected group of tested applications, and have limited functionality. If a smartphone is by any means an exemplar for consumers' attitudes towards technology, functionality seems one of the main elements attracting users. The attractiveness of smartphones is measured partly by the number of third party applications that are made available to it. The app store of Apple has over one million applications (Ingraham 2013), which seem far too many to vet properly, and should be a red herring for anyone using smartphones, and wanting to use third party applications. Consumers may also fail to assign the proper weight to ethical values and overvalue convenience or entertainment. A device that records data solely to convenience the lifelogger, e.g. helps the lifelogger retrieve his keys or captures people that are sexually attracted to him, can fail to promote any ethically relevant values.[65] However it does not seem unlikely that just those lifelog applications would make lifelog technology popular.

5) Sometimes it might be the vulnerabilities in the security of lifelog devices or applications that threatens control over the creation of data. Data can be created because external parties tamper with the functioning of devices. The connectivity of devices to the Internet exposes them to security risks. The FBI details the sentencing of a man who gained control over webcams, so he could blackmail the persons whom he covertly recorded (Christensen & Williams 2011). Another example is a documented plan of the NSA to infect

---

[65] Pupil dilation that can be captured with a high end camera can predict sexual orientation quite accurately (Rieger & Savin-Williams 2012).

computers with malware with the aim of controlling their microphones and webcams (Gallagher & Greenwald 2014).

Some insecurity arises from underfunding and hasty development. An example of sloppy programming by Apple could allow others to access login details and compromise connections to secure sites. The bug was the result of a single repeated line of code (Arthur 2014). The required expertise to develop secure applications is expected to be financially costly as well, as it slows down the release of the product and the agility of the company. In a highly unregulated industry in which start-ups can be underfunded while the pressure to release a product speedily is strong, it is unlikely that companies will hire the required expertise.

5) The lifelogger should be informed of many aspects involved in the functioning of lifelog applications and devices. However it often seems contrary to the short-term interests of lifelog companies to properly inform the lifelogger of the distribution of lifelog information and the risks expected from lifelogs. Transparency makes marketing efforts to position the device favourably in the market while optimising avenues for revenue more difficult. Security issues, access to and distribution of personal data, and commercially driven search results, seem little attractive for consumers, but are ethically relevant. Trading personal data and the use of personal data for advertising can be core strategies to generate revenue while these strategies might be unappealing to consumers. In addition, selecting the relevant information and presenting it in a comprehensible way is complicated and time consuming. In the long term, denying consumers protection against privacy infringements might be costly as it will erode trust.

Conclusion: In order to protect the lifelogger's privacy, the lifelogger should be informed of the data created and stored by lifelog devices, and of how they are used in a way that is understandable to them. Moreover, developers should secure lifelogs against third parties. However, the manifold of parties that can be involved in the development and commercialisation of lifelog technology and their interests can conflict with the need for transparency.

4.2.3.2 Concerns regarding access and distribution of information
Besides lacking control over the data created by lifelogs, the lifelogger can also lack control over the access and distribution of data.

The kind of storage used for a lifelog can aggravate these concerns. Some lifelogs, such as the one in the scenario (*2.5 Scenario*), might use clouds, which means that the main body of data is not in the physical possession of the lifelogger, but available through a network, usually the Internet. The servers on which these data are stored might be located in another country and outside the reach of the lifelogger. Connectivity to the Internet makes the lifelog vulnerable to second and third party access, as this network is accessible virtually from anywhere at any time. The transmission of data – e.g. Man-in-the-Middle attacks (MitM) – as well as the physical storage of data - e.g. remote access to data servers - could jeopardise lifeloggers' control over the access and distribution of their data. These data can be accessed and distributed legally through purchases and seizures or extrajudicially by hackers, rogue government agencies, or corporations wanting to make a profit.[66]

1) Lifelog companies may distribute lifelog data. Companies that offer lifelog services can offer these services on their own servers. By using clouds, these companies are the gatekeepers consumers have to pass to access data about their personal lives. Ethical issues with privacy can arise when corporations share data with third parties for commercial gain. This is more likely to happen when the ownership of data is solely or partly assigned to the company, or the purposes of use are insufficiently clarified, such as whether they have the legal authority to sell data to other companies.[67] Applications or devices can fail to create clear privacy policies, and often lack the incentive to provide protective privacy policies (the

---

[66] Recent revelations have shown that the legality of some surveillance programmes is disputable or unclear which is the case for some programmes of the US NSA (National Security Agency) and that corporations might knowingly hand over more data than they are legally required to (Ackerman & Roberts 2013; Ball 2013; Ball, Harding & Garside 2013). Moreover, the server can be stored virtually anywhere with a reliable Internet connection; the companies can choose a jurisdiction with data regulation laws in their (short-term) favour.

[67] However, one should not underestimate the power of consumers. It is unlikely that a critical mass of consumers would use services containing lifelog data which they would not own and which has no restrictions on use for other purposes. Even though individual consumers can always fall prey to such rogue services which may have been lacking public scrutiny, the ownership of data may be considered less important when services require personal information of which the occurrence of potential negative consequences appears only distant such as email addresses or even page views. This does not rule out companies such as Acxiom, which sells personal information but obtain it without explicit permission of the consumer. Acxiom gathers information which "includes biographical facts, like education level, marital status and number of children in a household; homeownership status, including mortgage amount and property size; vehicle details, like the make, model and year; and economic data, like whether a household member is an active investor with a portfolio greater than $150,000" (Singer 2013). These companies can apparently function without being stopped by data protection. The lifelog contains information that is so explicitly personal that issues of ownership will inevitably be raised by either the public, social media or traditional media. The popular outcry over changes in the terms of use of Instagram showed that consumers and media have the wits to avoid companies which do not provide them with ownership over their content hinting on the existence of a threshold which companies should not cross (Gross 2012; Smith 2013).

application or device can profit from the usage and sale of personal information). As a result, third parties could possess vast troves of personal information. Some data brokers claim to have data on almost every US household (Datalogix 2014) while others claim to have the profiles of approximately 700 million people (Acxiom 2013). Meanwhile, these data brokers eschewed to reveal from whom they acquired these data (Johnston 2013). The permission to use personal information for other purposes than initially intended might be gained over time. Companies could deploy bait-and-switch tactics (Meyer 2012). Initially consumers are lured under favourable privacy conditions. These conditions change when a critical mass of users dependent on the service is established. Switching services might be costly as one might have to give up years of lifelogging data.

Some lifelog companies might opt to sell their data de-identified, and in bulk largely intending to preserve the privacy of individual users. However, there is a risk that data can at later stages or through cross-linking be attributed to individual users, which makes the selling of bunk data a potential risk to privacy. Even anonymised information can sometimes be attributed to a specific individual (Ohm 2009). By using the data about anonymised web search queries shared by AOL, it was possible to identify people based on their searches alone (Barbaro & Zeller 2006). Sweeney found that 87% of the US populations "had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}" (Sweeney 2000, 2). Finally, Narayanan and Shmatikov (2009) found that they could de-anonymise 88% of the people both having the social networking sites Flickr (website for photo sharing), and Twitter.

2) In other cases even when the original corporation has policies in place to protect the privacy of its customers, the company could go bankrupt or it could be bought by another party allowing others that show less care for privacy access to the data of its customers.[68] Mergers can have an additional undesirable consequence, namely that companies can come to hold more information. Nissenbaum (2004b) has identified this as a potential issue. One piece

---

[68] For example, the $19 billion acquisition of Whatsapp, a messenger services predominantly available on smartphones, by Facebook shows that it might be difficult to rely on services in the long term (Albergotti, MacMillan, & Rusli 2014). Although Whatsapp's privacy policies might not have been altogether beneficial to privacy as Whatsapp stores information such as the telephone number of its users and the phone number from their address book on servers in the United States (Persson 2014). The developers behind WhatsApp positioned their application as an application that was adverse to advertisement as to provide advertisement companies would have to collect and process their users' data improperly and they would waste resources on data-mining instead of improving their service (Koum 2012). The take-over by Facebook means that advertisements with the additional costs are likely to become a reality at some point in the future.

of information may be relatively worthless on its own but assemblages and compilations of individual pieces of otherwise worthless information can reveal much personal information about an individual. According to her, data brokers make their money by piecing together pieces of information to create a greater understanding about an individual.

3) Lifelog companies can have their data subpoenaed by government agencies. Sometimes corporations are legally obliged to share their information with the authorities because they are bound by legalisation that sets limits to confidentiality. The revelations by Edward Snowden (Ball, Borger & Greenwald 2013) about secret services showed that corporations are sometimes put under pressure by governmental agencies to share some of their data. Although the capabilities and activities of intelligence agencies are often obscure, there is some indication that several member states of the European Union co-operate with US surveillance programmes or similar programmes which involve the sharing of information about innocent citizens, possibly violating human rights (Committee on Civil Liberties, Justice and Home Affairs 2013).[69]

4) The security of lifelogs might fail. Sloppy programming or yet undiscovered weaknesses in the infrastructure of the lifelog might create vulnerabilities of which malevolent others can profit. Sometimes these vulnerabilities are purposely created. Recent revelations about US and UK governmental agencies have shown that governments can show little restraint when accessing information. The NSA and the UK Government Communications Headquarters (GCHQ) have partnered with technology companies and Internet service providers to insert vulnerabilities into commercial encryption software (Ball, Borger & Greenwald 2013). The US and UK governments purposely build in weaknesses within encryption of secure data to make data more easily accessible to them (Ball, Borger, Greenwald 2013; Rushe 2013). Even storing the main body of data on a storage disconnected from the Internet may not prove adequate as there are ways to access computers that are

---

[69] The data obtained can be shared between institutions within a country as well as between countries. There was some controversy over the international sharing of SWIFT, which is a database that contains the bank transactions between approximately 8000 financial institutions, transactions between the United States of America and the European Union in 2006 and again in 2009 (European Commission 2010). Later the US targeted SWIFT and other financial institutions without their corporation (Spiegel 2013). Also individual member states share information such as the Dutch secret services (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten 2014).

offline. The NSA applied radio frequency technology to access computers not connected to the Internet (Sanger & Shanker 2014).[70]

When lifelogs are used on a broad scale, authorities are expected to attempt to obtain structural access to this source of information, for example by building in backdoors or requiring structural access to data from companies that store lifelog data. Currently, governments show little reticence in accessing personal information and it seems unlikely that they will restrain themselves from accessing lifelogs if they become mainstream. Lifelogs might become a tool for mass surveillance and to target specific individuals, such as activists or religious conservatists (see for more information *Diminishments by governmental agencies*). Even citizens might request access to check upon each other, something which will be discussed below (*4.2.3.4 Concerns with enforced access*).[71]

5) There may also be other kinds of structural issues. The applications offering access to lifelog data might have little incentive to protect the lifelog against third party access. As so many actors can be involved in the design and operation of lifelog technology, individual actors might be little inclined to take up the burden of securing the lifelog. In addition the novelty of the technology and the device might mean that there are no third parties specialised in security such as those offering virus scanners and firewalls on laptop computers. Also, companies offering cloud storage may offer employees access to the cloud or may provide other customers accidentally with access to data, as has happened before (Barton 2012; McMillan 2013).

Conclusion: The fact that lifelog data could be shared without the lifelogger being notified decreases his control over his personal information. The spread of data to and between individuals, corporations, or governmental institutions can impair one's ability to

---

[70] Although the latter would require more effort as it might require physical proximity to the target so it is likely only done under special circumstances when someone has a strong incentive to access the computer. Therefore, the majority would be protected.

[71] Even fellow citizens might use lifelogs for surveillance; they might require access to the lifelog to watch over the behaviour of the lifelogger, such as jealous spouse checking up on their partners. (This is discussed in more detail in *4.2.3.4 Concerns with enforced access*.) Sometimes it is actually a distrustful partner who as a governmental official checks the behaviour of her partner. The NSA mentioned a data analyst who tasked her husband's cellular phone to check if he was faithful instead of others using her authority to secure the national interests. This was revealed in a letter from the NSA Inspector General Ellard to Senator Charles Grassley. This letter is available from: http://www.documentcloud.org/documents/799762-nsa-surveillance-09-11-13-response-from-ig-to.html#pages/p1. Another risk to privacy is posed by private citizens accessing lifelogs illegitimately. Personal information can serve different purposes. For example, malevolent hackers could try to access lifelogs because of the financial worth of personal information and the opportunities it offers for fraud, theft or extortion.

correct personal information. Indeed, the companies or authorities that purchase or seize these personal data could distribute these data as well. Sometimes information that is being spread is false. A notable example of a false positive was when Edward M. Kennedy, Democratic Senator of Massachusetts, was refused to board a plane because his name was similar to an alias used by a suspected terrorist (Swarns 2004). It turned out that even for Kennedy, a well-known and influential figure, the placements on the Terrorist Watchlist and corresponding no-fly lists were difficult to correct, as was shown when he was again refused to board a plane on another occasion a few weeks after the first incident.

Access by third parties is often obscure, especially when these data are controlled by the lifelog company, leaving lifeloggers with little certainty about the extent to which others possess and distribute their personal data. Storing personal information outside the control of lifelog companies would at least make mass seizures of data more difficult, and it may protect the lifelogger against companies sharing their information. Another measure is to secure lifelog content against other parties than the lifelogger accessing it. However, to categorically exclude others from accessing a lifelog is difficult to achieve and can be costly. In addition, there are legal limitations on the confidentiality of data.

4.2.3.3   Concerns regarding the usage of data

The ease of distribution facilitates the use of lifelog data for other purposes than to provide the lifelogger with an insight into his life. The trove of personal data contained in a lifelog can be a very valuable asset to achieve other goals than providing the lifelogger with information about his past such as advertisement and surveillance. Even if the storing of information on corporate servers constitutes no violation of privacy, the use of data for other purposes might.

Infringements of privacy are not always dependent on the distribution of personal information to other parties. Sometimes it is the usage of data rather than the distribution of information, which violates privacy. Although Facebook does not let advertisers access personal information directly, it did stir controversy when revealing that they wanted to create social advertisements by using people's 'likes' as recommendations (Kafka 2011; Margaris 2012). These 'likes' on Facebook by the member of Facebook are not necessarily meant as an endorsement of a brand or a product, as members sometimes do it for promotions or for apparently no reason at all (Protalinski 2012). The use of likes led to embarrassing situations. Nick Bergus jokingly liked a product page on Amazon – a web shop – by

highlighting a webpage advertising a gallon of lubricant. His 'like' got promoted by Facebook to his 'friends', including the wife of a co-worker and a former employer (Sengupta 2012).[72] Even though these likes were not shown to anyone who did not already have access to this information, the use of this information for other purposes can provide this action with different and unintended connotations that can be inappropriate. Another kind of misuse, also by Facebook, was to manipulate the posts on the News Feed of a large set of users to test if there was emotional contagion (for more details see *5.2.1.2 Persuasion/Manipulation*).

Conclusion: Lifelog data could be used for many purposes of which some would reduce or violate the privacy of the lifelogger. In order to prevent this from occurring lifelogs should be secured against third party access, and the purposes for which companies offering lifelogging services and products can use the data should be appropriate, well-defined, and limited. One way of achieving this is to ensure that the lifelogger has all or most of the personal information from the lifelog in his possession so that it cannot be used by others without her consent.

4.2.3.4 Concerns with enforced access

There are also ways in which privacy can be reduced or violated through lifelogs which are mostly irrespective of the design and security of lifelog technology.

1) Similar to diaries, lifelogs are vulnerable to being accessed by people within one's vicinity. These could be fellow members of one's social environment. For instance, if the lifelogger leaves the interface to query a lifelog opened on the browser, the lifelog becomes accessible to people using the computing device after the lifelogger. The open browser would be comparable to a diary left readily accessible in one's room. Also, one can be forced to keep a lifelog or provide access to it by people within one's vicinity, such as a distrustful spouse or parents wanting to check the behaviour of their significant other or their children. The result would be that the lifelogger has little privacy.

---

[72] Currently, Facebook has provided the option to opt-out of using likes for advertisements. Facebook's Beacon was another advertisement programme in which Facebook got information about their members' activities on third party websites even when they indicated that they did not want their results published on their Facebook feed and when they were logged off. Also, the service was not transparent enough which led to people publishing their purchases such as video rentals and booked holidays without realising it (Perez 2007). It was an opt-out system (Story 2007). At the time of writing, 03-12-2013, it was possible for an individual member to prevent Facebook from using 'likes' to advertise products to friends.

2) Governmental agencies and corporations may request access to a lifelog. There have been cases of employers or interviewers who have demanded access to a (potential) employee's social network. For example, an Air New Zealand flight attendant was fired from the company when she refused to grant her employer access to her bank details and Facebook account. Her employer suspected her to have misused her sick leave which she used to assist her sister in the final stages of her pregnancy (Kensington v. Air New Zealand Limited 2013). When she appealed the decision, her employer requested access to her financial details and her Facebook account. She refused, but the Employment Relations Authority (ERA), which is an independent governmental body to resolve issues in employment relations, allowed the national airline of New Zealand to access this information even when she handed over written reports by the midwife, her sister and husband. Her Facebook and her financial details were, according to the ERA, a fair means to obtain evidence. Further investigation led the ERA to conclude that the employee rightly took her sick leave although it also concluded that the investigation including the requested access to Facebook was fair (Kensington v. Air New Zealand Limited 2013). There are also cases in which governments are allowed to access digital information through user-interfaces. For instance, in the US the government is allowed to conduct intrusive searches into electronic devices and confiscate them even without any suspicion of illegal wrongdoing as a recent court ruling revealed (Abidor v. Napolitano 2013).

Indeed, as will be discussed later (*7.2.3 Being free*), in case lifelog technology becomes widespread and one can reasonably be expected to have lifelog information to one's avail, one may be forced to hand over one's own personal information more frequently. Imagine cases in which an insurance company can offer variable quotes or coverage based on behaviour. Already there is legislation in some countries that allows such discriminations. In the US, employers are allowed to offer their employees variable health insurance rates determined by wellness-related choices, such as dietary choices and physical exercise (see the U.S. Patient Protection and Affordable Care Act (PPACA)). Such demands for information are expected to be most frequently made in cases in which there are financial and/or other material and measurable interests at play, which was the case with rewarding or penalising particular health-related behaviour, and one could imagine other situations such as benefit fraud. For these interests, the request to access lifelog information might be defended by referring to the gains that can be made, and the undesirability of the penalised or the desirability of the incentivised behaviour.

Conclusion: One may experience reductions of privacy regardless of the security of lifelogs. There seems to be no straightforward way in which lifeloggers can be protected against authorities demanding personal information when they have the legal right to do so. Also when access is demanded within the family or by acquaintances, there seems no evident protection. Just as parents could check upon their children's goings-on by reading their diary without legal repercussions, they could also access lifelogs. Perhaps the severe consequences of a lack of privacy warrant some protection against imposed access or the forced keeping of lifelogs, as it may be considered a form of abuse. Moreover, it is probable that most people will find it inappropriate to access someone else's lifelog and will refrain from either forcing someone to lifelog or access the other's lifelog when it is available to them.

With regard to employers, it seems unlikely that there would be no legal limitations in place that forbid companies to access the lifelogs of its employees without some legal procedure, although the procedures might be lax in granting sufficient protection, which was arguably the case in the example of Air New Zealand. In most countries, the rule of law will limit the access of, future, employers to lifelogs. Similarly, citizens would often have some protection against government officials commanding access to electronic devices although this protection can be inadequate, as is arguably the case around the US border. This issue is at least partly dependent on the legal system in place and will vary across jurisdictions.

4.3 Opportunities for privacy

There may be some minor advantages to lifelogs with regard to control.

Lifelogs can be used to provide people with information about themselves that currently is only available to government agencies, public institutions or corporations. For instance, government agencies have the capacity to gather personal information from multiple sources, digital and non-digital, and process that information. Citizens are likely to have fewer resources and time to access and process these on the same scale and with the same effort as government agencies. Consequently, governmental authorities may actually have more information about individuals, than those individuals have about themselves. Lifelogs provide a counterbalance against the power of authorities by providing lifeloggers with information to correct erroneous personal information in the hands of an authority. The same applies more or less to other public and/or private institutions such as hospitals and medical clinics. Before the advent of wearable sensor devices for consumers, they were the only gatekeepers of information about one's health. The ability to capture information allows

persons to access and interpret their own personal information, and form a greater understanding about their conditions without having to depend on healthcare professionals.[73]

In some situations, lifelogs can also support people correct existing misconceptions about them in their social environment. It has already been identified as an advantage in the discussion on the ethics of lifelog technology that the use of lifelogs can be a tool for the correction of information about the lifelogger and shape other people's impression of the lifelogger (O'Hara, Tuffield & Shadbolt 2009). However, the reach of this advantage is limited. Certain conditions need to be fulfilled in order to correct such information: it needs to be possible to refute or correct this kind of information, while some information cannot be refuted, such as information that is factually correct but outdated; one needs to have a platform to reach the target audience; the target audience must be prepared to listen; and one must be aware of the existence of this false information. Also, these conditions have to be fulfilled during the period of time that this information can surface. If these conditions are left unfulfilled, having the information necessary – one of the conditions, but by itself insufficient – would be superfluous. Often this will be the case. For example, the spread of a video that has been shared on a public website and is attracting mass attention – it has gone viral. Suppose as well that the video is edited to paint an unfavourable picture of the person portrayed – by cutting some of the footages in which the person is made to look like an aggressive drunkard – but factually correct – the person was intoxicated and accidentally too rough. That person would have a hard time putting this information into the right context. Even if the person depicted is aware of all the other platforms that have copied and shared the video – a feat which is practically infeasible for ordinary people – then some platforms might not offer the facility for correction or removal. Furthermore, those watching the video might have no interest in a correct portrayal; they might want to be entertained only. Indeed, a balanced account might only interfere with their interest by taking away the enjoyment. Finally, the interpretation of information is hard to control, making it difficult to correct information as information could be interpreted in a different sense than was intended. This issue was already examined by Bailey and Kerr (2007) in relation to the Ringley case.

---

[73] However, one would need a healthcare system willing and allowed to accept such data and the data need to have an acceptable standard, both of which require positive actions. This has also downsides in this particular case such as increased medicalisation and a lack of infrastructure and maybe quality product to allow such data to be useful rather than a burden. This is further discussed in the chapter on beneficence.

Conclusion: These characteristics of lifelogs actually speak in favour of lifelogs. However, the advantage they offer seem little significant compared to the potential issues associated with lifelog technology and privacy, especially because the advantage only occurs under quite specific circumstances. The advantage seems to neither negate nor outweigh the issues with privacy identified before.

4.4   Extenuating circumstances

There are also extenuating circumstances that contextualise the above mentioned issues with regard to privacy. The points discussed in this section are not meant to justify the risks to privacy or refute the harms to privacy. They are solely meant to show factors that to some extent lower the weight of the consequences of the use of lifelog technology for the privacy of lifeloggers and non-lifeloggers.

4.4.1   Plenitude of data gathering devices

Although lifelogging devices seem to have the potential to reduce privacy and can be used to violate privacy, they are not the sole devices to do so. The marginal costs of lifelog technologies might be minor considering the environment in which they will function. In current Western societies, people have immersed themselves or are immersed with technology that has the capability to capture and store personal data. The data that are already captured include use of public transport, bank transactions, credit card transactions, flight information, birth certificates, housing situation, education, income, insurance, telephone records, CCTV in public places, audio recordings in public places, medical records, employment histories, emails, social contacts, search queries, data from social networking sites, *et cetera*. In most areas of daily life in which the principle to respect privacy is considered to merit some weight, technology that captures and digitises information is already deployed. These data can pose a risk to privacy. Companies can fail to secure the data in their possession properly, sell them, use them for other purposes, *et cetera*. In addition, both governmental authorities and corporations have shown an interest in accessing and/or gathering these data. In such an environment, targeting individual technologies seems an insufficient and makeshift measure, if one is concerned about privacy. This is especially the case with lifelogs, since one can create them from devices that are already widely used, and

other parties might be doing just that anyway, but outside one's control.[74] The, sometimes small and often uncorrelated, steps taken by recording and digitising services, and activities have led to a situation in which lifelogs are the next small step in reducing privacy.[75] This is not to argue that lifelog technology is not undesirable for privacy. It merely contextualises the issues with privacy.

Conclusion: In the current environment, the reductions and violations of privacy caused by other technology slightly reduce the effect of lifelogs on privacy. After all, digital data can already reveal information about many areas of daily life. The effect of lifelogs is predominantly one of scope as many activities already leave digital traces.

4.4.2 Existing moral, social and legal norms

Despite all these opportunities for capturing and sharing information about each other, people often seem to successfully rely on the safeguards in place to protect privacy. This is partly explained by the fact that there are moral, social, and legal norms in place. People often refrain from recording each other, and share personal data, because they consider the sharing unethical, or they could be punished for it socially or legally. Also, people may find some parts of their lives unsuited to be recorded. For these reasons, it seems that sometimes one can successfully rely on social, legal, and moral norms for privacy.

This is not to state that social or legal norms are sufficient. Social norms alone seem inadequate for safeguarding privacy. The dependence on the discretion of the lifelogger is a thin base on which to sustain privacy and therefore insufficient in numerous contexts. In enclosed social circles in which contact between members is reoccurring, e.g. between colleagues sharing an office or with close acquaintances, it is reasonable to expect that people come to some mutual agreement, which allows one to presume some privacy. Situated in an open and heterogeneous society, one often has to rely on strangers. This brings an element of uncertainty, as conceptions of privacy can differ. The norms of appropriateness are largely cultural, for example the Ssengas in Uganda whose paternal aunts teach their nieces the movements to be performed in the bedroom after marriage, an openness which one would typically be unfamiliar with in most Western cultures (Nakazibwe 2012). Sometimes people might misinterpret the situation, or unintentionally or accidentally capture information while

---

[74] Moreover, others such as government agencies and corporations could create lifelogs using this information leaving only the individuals without the same functionality. Lifelogs would put individuals on equal footing with authorities.

[75] The fact that privacy can be diminished through small and by itself marginal steps is another issue.

lifelogging, for instance tourists failing to recognise a situation. And indeed, some people might be blatantly indifferent to the worth of privacy.

Moreover, these norms are subject to change and it is currently unclear how lifelogs affect social norms. It is possible that one can get progressively accustomed to lower levels of privacy. Existing norms might gradually change because of the introduction of novel technology. After all, it is questionable whether one had chosen to share so much information about onself and others with other citizens, corporations, and the government only a few decades ago.

In addition, the recent revelations about government agencies snooping data show that either the legal protection of privacy is lacking or badly complied with offering little protection for privacy. Moreover, the legal framework in which citizens and corporations can gather and share data leaves much space for reductions or violations of privacy. Strict adherence to the law seems insufficient to safeguard the privacy of the citizens.

Conclusion: The potential of lifelogs to violate or reduce privacy will be somewhat tempered by social and legal norms, but these seem insufficient to safeguard privacy.

4.5 Summary

It is evident that lifelogs can pose risks to a lifelogger's privacy and the privacy of others. Indeed, they potentially have the capability to negatively affect many of the conditions necessary to safeguard privacy. The above showed that one's ability to manage one's privacy – partly determined by the opportunities to correct, choose or consent to information being revealed and distributed- can be severely diminished with the digitisation of information by lifelog technology. In addition, lifelogs might reveal or distribute personal information inappropriately.

The manners in which lifelogs can increase personal information have been discussed. Personal information for the lifelog is created by (1) changing the functionality of ordinary devices and turning them into lifelogging devices, such as the smartphone, (2) the development of devices especially for lifelogs, (3) creating novel information from existing sources of data, and (4) the bundling of data sources. The fact that lifelogs capture and create information autonomously without human interference, and collect and process several data sources allows for the revelation and distribution of information that was impossible to be captured previously before the advent of lifelog technology. Digital information has an

advantage to analogue information with respect to the fact that certain limitations to the distribution of information are alleviated.

Several privacy-related concerns have been identified. Lifeloggers might obtain access to personal information about others outside the control of these people recorded. Improved retrieval technologies and high-end sensors can aggravate these issues. One concern for privacy is that lifelog devices could reduce people's expectation of privacy in some situations. Additionally, strategies that rely on the discretion of the lifelogger to respect the privacy of others when using recording devices seem flawed for different reasons. In addition, the lifelogger may have little control over the creation and utilisation of data by other parties and the access and distribution of information. Against these concerns, it might be argued that people already experienced major reductions of privacy, but this makes the potential negative effects of lifelogs on privacy not undesirable. Violations of privacy are undesirable regardless of other reductions or violations. Also, one could argue that through lifelogs, lifeloggers can correct misconceptions held by others about them, but this advantage seems too minor to hold up against the potential loss of control over personal information.

Many of the issues regarding privacy are alleviated or solved by (1) securing the lifelog against third party interference to ensure that the lifelogger is the sole possessor of personal information, (2) avoiding devices and applications that capture data that can refer to other people than the lifelogger, and (3) strictly defining and limiting the purposes for which information can be used, which should be ethical in nature. However, these goals are nearly impossible to achieve completely. Perfect security is as yet non-existent, and even if there were a way to secure the technology from others accessing it, there would still be legal limitations on confidentiality or to the risk of people physically enforcing access to lifelogs' content. In addition, the current state of lifelog technology seems to indicate that information about others is considered an integral part of lifelogs. After all, an overview of someone's past would be severely lacking without information about others, as others form part of one's life. Also, reducing lifelog content to sources that only reveal information about the lifelogger would severely impair functionality; many data sources that can reveal personal information about the lifelogger may also reveal information about others. In addition, companies involved in lifelogging may have little incentive to limit the purposes for which personal data can be used.

4.6   Recommendations

In this part of the thesis, recommendations for developers to mitigate or meet concerns regarding privacy are discussed. Privacy concerns are partly dependent on the design of the lifelog. In order to minimise the issues identified, ten recommendations are provided to protect privacy. These recommendations predominantly are determined by ways to maximise control and limitations to which data can be used.[76]

1. <u>Minimise information that can refer to others:</u> Information about others should be avoided to the greatest extent possible. If data about others are necessary for the functioning or adoption of the technology, the form in which the data are presented has to be considered. Data can be presented in various ways, photos can be fed back to the lifelogger by only providing metadata or blurring the images of others (e.g. MPEG-7 with privacy protection mask is a data format designed to protect privacy by default (Eptascape Inc. 2010), or a combination of metadata, censored data, and original data depending on the situation, or the lifelogger can be presented with photos in which there are no people. Many issues with privacy are solved by limiting the retrieval of information, so even developers could choose not to allow the retrieval of particular information. The need for specific recognition technologies should be critically assessed, especially features such as identification technology and emotion recognition technology which are of concern to privacy.

2. <u>Informing individuals recorded by the lifelogger:</u> To minimise privacy concerns, the lifelogger should inform others to the greatest extent possible that he is recording them. An integral part of privacy is the ability to choose privacy. In order to sustain privacy, it is recommended that lifelog devices and applications indicate that they are recording. This can be as simple as integrating a light in the design to show others that the device is recording. The same technology is used in video recorders equipped with recording lights, and on the Vicon Revue. One could even think of low tech solutions that make it more apparent that a device is not recording, such as physically covering the lens of the camera or allowing one to take out the battery ensuring the device cannot function anymore.

3. <u>Control over storage:</u> Both the lifelogger and the persons he captures should have the opportunity to determine the data and information retrievable in a lifelog to the

---

[76] Some recommendations can be found in Jacquemard et al. 2014.

greatest extent possible.[77] Both should have a choice whether they want this information to appear, although this will be hard to achieve for those who are captured by the lifelogger.[78] A lifelog should provide optimal transparency with regard to what data it contains. Any attempts to obscure this transparency may be deemed unethical. In addition, the lifelogger should be able to remove data, and these deletions should not be retrievable. Ideally, the person being recorded has the same ability. The ability to remove data and information is essential for control. One reason is that the lifelogger may think that some data or information is or has become inappropriate. When the data are indiscriminately and permanently kept or stored in a lifelog or copied to other databases, this would severely diminish the lifelogger's control over the dataset. Finally and most importantly, the lifelogger should always be able to request the data about him that is in the possession of the lifelogging company and the lifelogger should never be forced to keep a lifelog by the company.

4. <u>Control over recording:</u> The lifelogger should be able to select the data sources that collect data, which can convey personal information about them, to the greatest extent possible. Moreover, the lifelogger should be able to stop recording with a minimum of effort, as situations can change abruptly, and the recording can become a violation of privacy. Both the Narrative Clip and the Vicon Revue lacked a pause or stop function in their first design, and the Narrative Clip (Memoto 2013) is still lacking this feature. Again, low tech solutions might be useful, such as the ability to physically cover the lens of the camera or the microphone or allowing one to take out the battery. Moreover, the need for specific data needs to be assessed. Keeping data sources to a minimum would be preferable.

---

[77] Increasing the scope for consent might be difficult but not impossible. To build in a time delay before any captured information is stored permanently provides people at least with an option to voice their dissent. Another solution would be to equip devices such as smartphones with identifiers that indicate that a person does not want to be captured. A database may be established of people who have requested that their information should not be logged by others. Although these solutions are not ideal as they require opt-out rather than opt-in, they soften privacy concerns to some extent. A better solution would be to design an opt-in system which may consist of a database of persons who have agreed that their information *can* be used. Only information about people who have opted in will be captured, stored and may be retrieved.

[78] A lifelog device could also function as traditional photo camera in the sense that one should press a button to gain access to the specific images, or else the device only provides metadata or censored information. For example, developers could add a button, which makes the photos of a minute ago available. One could also suggest the reverse; add a button which prevents the storage of photos from a set amount of minutes beforehand. This way one could prevent the storage of information that one did not intend to capture.

5. <u>Ability to correct data:</u> The lifelogger should be able to modify the information, which is stored in a lifelog. Ideally, others recorded by the lifelogger have the same ability, but there seems to be no evident way to achieve this. This can take different forms. One of them is the ability to correct erroneous information. Lifeloggers should have the opportunity to correct information especially in case it could be distributed to other parties. Also, the lifelogger should be able to annotate and change information, as he may feel this information provides an unfair image of him, or the availability of this information is contrary to his conception of appropriateness.

6. <u>Possession of lifelog data:</u> The possession of personal lifelog data about the lifelogger by other parties than the lifelogger should be minimised. The company offering a lifelog application or device may have their data subpoenaed by government agencies without being allowed to inform the user. In addition, when companies do not have data in their possession, they evidently cannot sell them or hand them over. A single data server containing information about numerous lifeloggers is more interesting to third parties than numerous personally held storage drives containing the data of only one lifelogger and maybe his family's.

7. <u>Legal clarity:</u> The ownership of data, including activities arising from ownership such as the licensing of lifelog data, should be determined and communicated clearly to the lifelogger to avoid confusion. It should be clear what happens when the lifelogger wants to remove the lifelog altogether, or passes away, or when the company changes ownership or files for bankruptcy. In addition, limitations to the goals of data use should be formulated and communicated clearly to the lifelogger. Comprehensive but understandable 'terms of use' and/or 'legal terms' - similar to plain language statements for research trials - are paramount but difficult, due to the multitude of lifeloggers with different levels of competence, and even competent persons can have issues regarding providing consent. Finally, philosophical discussions on the issues of ownership are encouraged, as the current regulation can be ethically insufficient or unethical.

8. <u>Security:</u> The fact that lifelogs should be secure against second party (i.e. the lifelog company) and third party access, first and foremost seems an integral part of the lifelog, which should need no further explanation. Developers should hold security at the highest esteem, and incorporate it at the heart of their design. Some security

concerns arise from storage. Cloud computing could create issues, as the connection to the Internet leaves the lifelog particularly vulnerable to third party access. Ideally, the information would not be stored on corporate servers, but the data should be in the possession of the lifelogger. Privacy enhancing technologies (PETs) could be useful. Also, the encryption of files may provide some additional security. End-to-end encryption that encrypts data from sender to recipient would be especially useful. Furthermore, lifelogs could be equipped with a timer that requires the lifelogger to log in again after a set amount of time within which the interface to the lifelog has not been used. The chance that others access the lifelog when a lifelogger forgets to log out is minimised by such a measure.

9. <u>Review third parties applications and devices:</u> The addition of third party applications and devices could weaken privacy. These parties may not hold the same standards for privacy as other companies. It is recommendable to vet third party applications that are offered through official channels of the lifelog company. Evidently lifelog companies cannot prevent lifeloggers to manually add third party applications by themselves, but they could inform their users that these applications pose additional risks.

10. <u>The purposes used:</u> The lifelogger should (a) be informed about the use of his personal content for other purposes than to provide him with information about his past, and (b) these purposes should be legally, morally, and socially acceptable. Even without sharing or accessing personal data, lifelog technology can infringe on the privacy of the lifelogger. New uses for lifelog data should be introduced with the free consent of existing users. A situation should be avoided that lifeloggers are forced to choose between losing lifelog functionality or even their lifelog data, or losing their privacy.

Lifelog applications and devices are unlikely to meet all privacy concerns. This is partly because the recommendations are often technically difficult to achieve and/or a perfect model to strive for rather than an achievable goal, e.g. perfect security is a commendable aim but as yet unattainable. Moreover, some of the recommendations might impair certain aspects of the functionality of lifelogs, and one may prefer using those functionalities rather than to addressing privacy. Also, some issues with privacy are inter-reliant on legislation or

responsible use, making the protection of privacy not only a case for the developer but also for the environment in which lifelogs are used.

4.7   Conclusion

In this chapter, privacy concerns with regard to lifelog technology have been presented and discussed. The definition of privacy used is based on the RALC theory as defined by Tavani and Moor (2001). They assert that privacy depends on both access and control.

After examining the effect of lifelogs on privacy, the conclusion is that the use of lifelog applications and lifelog devices will most likely impact privacy negatively. Indeed, designing lifelogs in a way that the privacy of lifeloggers remains completely unaffected seems unattainable as yet. By securing the lifelog against third party access, limiting the purposes to which lifelog data can be used, and by avoiding capturing information that can refer or be attributed to others, one could largely avoid issues regarding privacy. Also, a checklist has been provided to help developers identify privacy issues (*Appendix A: Checklist for privacy*).

In the last part, design recommendations have been provided to meet some of the challenges. The chapter is further expanded by offering recommendations so that lifelogs can be made to conform better to privacy. Following these recommendations will not negate all privacy concerns. If there were no *prima facie* principles that factor more forcefully in favour of the further development of lifelogs than the *prima facie* principle of respect for privacy against, then, based on respect for privacy alone, a halt to the further development of lifelog technology would be the ethically desirable way to proceed. Respect for privacy is a *prima facie* principle that factors against the further development of lifelog technology.

Bibliography

Aarts, E. & Marzano, S. 2003. *The New Everyday: Views on Ambient Intelligence*. Rotterdam: 010 Publishers.

Abidor v. Napolitano. 2013. ERK. 10-cv-04059.

Ackerman, S. & Roberts, D. 2013. NSA phone surveillance program likely unconstitutional, federal judge rules [Online]. *The Guardian.* Available from: http://www.theguardian.com/world/2013/dec/16/nsa-phone-surveillance-likely-unconstitutional-judge [Accessed 25-02-2014].

Acxiom. 2013. *Annual Report 2013* [Online]. Available from: http://investors.acxiom.com/secfiling.cfm?filingid=733269-13-12&cik= [Accessed 20-05-2014].

Albergotti, R., MacMillan, D., & Rusli, E.M. 2014. Facebook to pay $19 billion for WhatsApp [Online]. *The Wall Street Journal*. Available from: http://online.wsj.com/news/articles/SB10001424052702304914204579393452029288302 [Accessed 25-02-2014].

Allen, A.L. 1999-2000. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *32 Conn. L. Rev,* pp. 861-876.

Allen, A.L. 2008. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74.

Allen, A.L. 2011. Privacy and Medicine. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy. Spring 2011*. Available from: http://plato.stanford.edu/archives/spr2011/entries/privacy-medicine/Aristotles [Accessed 19-05-2013].

Allen, A.L. 2012. What Must We Hide?: The Ethics of Privacy and the Ethos of Disclosure. FALL 2012 Distinguished Speaker Series. Miami: St. Thomas University School of Law.

Aristotle.1984. *Politics*, translated by Jowett, B. Princeton: Princeton University Press.

Aristotle. 1998. *The Nicomachean ethics,* translated by Ross, W.D. Oxford: Oxford University Press.

Arthur, C. 2014. Apple's SSL iPhone vulnerability: how did it happen, and what next? [Online]. Available from: http://www.theguardian.com/technology/2014/feb/25/apples-ssl-iphone-vulnerability-how-did-it-happen-and-what-next [Accessed 20-03-2014].

Backstrom, L. & Kleinberg, J. 2014. Romantic Partnerships and the Dispersion of Social Ties: A Network Analysis of Relationship Status on Facebook. Proc. 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW) [Online]. Available from: http://arxiv.org/abs/1310.6753 [Accessed 02-04-2014].

Bailey, J. & Kerr, I.R. 2007. Seizing Control? The Experience Capture Experiments of Ringley & Mann. *Ethics and Information Technology*, 9(2), pp. 129-139.

Ball, J. 2013. Leaked memos reveal GCHQ efforts to keep mass surveillance secret [Online]. *The Guardian.* Available from: http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden [Accessed 07-03-2014].

Ball, J., Borger, J. & Greenwald, G. 2013. Revealed: how US and UK spy agencies defeat Internet privacy and security [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 09-09-2013].

Ball, J., Harding, L. & Garside, J. 2013. BT and Vodafone among telecoms companies passing details to GCHQ [Online]. *The Guardian*. Available from: http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq [07-03-2014].

Bannon, L. 2006. Forgetting as a Feature not a Bug. *CoDesign.* 2(1), pp. 3-15.

Bannon, L. 2011. Reimagining HCI: Toward a More Human-Centered Perspective. *Interactions*, 18(4), pp. 50-57.

Barbaro, M. & Zeller Jr., T. 2006. A Face Is Exposed for AOL Searcher No. 4417749 [Online]. *The New York Times.* Available from: http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0 [Accessed 09-12-2013].

Barton, M. 2012. How Safe Is Your Data Stored in Apple's iCloud? [Online]. *Wired.com*. Available from: http://www.wired.com/insights/2012/03/icloud-safe/?utm_source=pulsenews&utm_medium=referral&utm_campaign=Feed%253A+wired%252Findex+%2528Wired%253A+Index+3+%2528Top+Stories+2%2529%2529 [Accessed 19-05-2013].

BBC. 2003. Unique book goes on display [Online]. Available from: http://news.bbc.co.uk/2/hi/europe/2939362.stm [Accessed 14-01-2014].

Beauchamp, T.L. & Childress, J.F. 2009. *Principles of Biomedical Ethics: Sixth Edition*. New York & Oxford: Oxford University Press.Bilton, N. 2011. Tracking File Found in iPhones [Online]. *The New York Times*. Available from: http://www.nytimes.com/2011/04/21/business/21data.html?_r=0 [Accessed 29-01-2014].

Bohn, D. 2014. Google Glass just got a lot less geeky [Online]. *The Verge.* Available from: http://www.theverge.com/2014/1/28/5352592/google-glass-prescription-lenses-frames-titanium-collection [29-01-2014].

Byrne, D., Lavelle, B., Doherty, A., Jones, G. & Smeaton A.F. 2007. Using Bluetooth and GPS Metadata to Measure Event Similarity in SenseCam Images. *IMAI'07 - 5th International*

Conference on Intelligent Multimedia and Ambient Intelligence, Salt Lake City, Utah, 18-24 July, 2007.

Byrne, D, Kelly, L., & Jones, G.J.F. 2010. Multiple Multimodal Mobile Devices: Lessons Learned from Engineering Lifelog Solutions. In: Alencar P. and Cowan, D. 2012. *Handbook of Research on Mobile Software Engineering: Design, Implementation and Emergent Applications*, IGI Publishing.

Chen, Y. & Jones, G.J.F. 2012. What do people want from their lifelogs? *IN: 6th Irish Human Computer Interaction Conference*.

Christensen, S.S. & Williams, J.L. 2011. Orange County Man Who Admitted Hacking Into Personal Computers Sentenced to Six Years in Federal Prison for 'Sextortion' of Women and Teenage Girls [Online]. *FBI Los Angeles Division*. Available from: http://www.fbi.gov/losangeles/press-releases/2011/orange-county-man-who-admitted-hacking-into-personal-computers-sentenced-to-six-years-in-federal-prison-for-sextortion-of-women-and-teenage-girls [Accessed 17-12-2013].

Clowes, R.W. 2012. Hybrid Memory, Cognitive Technology and Self. *The proceedings of the AISB and IACAP World Congress 2012*.

Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten. 2014. *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD* [Online]. Available from: http://nieuwsuur.nl/documenten/ctivd_toezichtsrapport_1.pdf [Accessed 12-03-2014].

Committee on Civil Liberties, Justice and Home Affairs. 2013. *DRAFT REPORT on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* [Online]. Available from: http://statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf [Accessed 14-01-2014].

DARPA/IPTO. 2003. BAA # 03-30 *LifeLog Proposer Information Pamphlet* [Online]. Available from: http://realnews247.com/lifelog.htm [Accessed 30-01-2012].

Datalogix. 2014. *About us* [Online]. Available from: http://www.datalogix.com/about/ [Accessed 21-05-2014].

DeCew, J. 2013. Privacy. In E.N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy. Fall 2013*, Available from: http://plato.stanford.edu/archives/fall2013/entries/privacy/ [Accessed 23-12-2013].

Dijck, J. Van. 2012. *Mediated memories in the Digital Age*. Stanford: Stanford University Press.

Dodge, M. & Kitchin 2005. The ethics of forgetting in an age of pervasive computing. *CASA Working Papers 92*. London: Centre for Advanced Spatial Analysis.

Dodge, M. & Kitchin, R., 2007. Outlines of a world coming into existence': pervasive computing and the ethics of forgetting. *Environment and Planning B Planning and Design*, 34(3), pp.431-445.

Dodge, M. 2007. Do we need an ethics of forgetting in a world of digital 'memories for life'? *Position paper for Designing for Forgetting and Exclusion conference.*

Eede, Y. Van Den. 2011. Technological remembering/forgetting: A Faustian bargain? *Empedocles: European Journal for the Philosophy of Communication*, 2(2), pp. 167-180.

Eptascape Inc. 2010. *MPEG-7 Technology* [Online]. Available from: http://www.eptascape.com/products/mpeg7.html [Accessed 09-09-2014].

European Commission. 2010. EU prepares new negotiations with US government on transfer of bank data for purpose of fighting terrorism [Online]. Available from: http://ec.europa.eu/news/justice/100325_en.htm [Accessed 19-05-2013].

Fernandez, K. C., Levinson, C. A. & Rodebaugh, T. L. 2012. Profiling: Predicting Social Anxiety From Facebook Profiles. *Social Psychological and Personality Science*.

Fried, C. 1968. Privacy. *The Yale Law Journal*, 77(3), pp. 475-493.

Gallagher, R. & Greenwald, G. 2014. How the NSA Plans to Infect 'Millions' of Computers with Malware [Online]. *The Intercept.* Available from: https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 18-03-2014].

Gavison, R. 1980. Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), pp. 421-471.

Gellman, B. & Miller, G. 2013. U.S. spy network's successes, failures and objectives detailed in 'black budget' summary [Online]. *The Washington Post*. Available from: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html [Accessed 09-09-2013].

Gellman, B. & Soltani, A. 2013. NSA tracking cellphone locations worldwide, Snowden documents show [Online]. *The Washington Post*. Available from: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [Accessed 13-12-2013].

Giudice, K. Del. & Gardner, M. 2009. *The Message of the Pensieve: Realizing Memories through the World Wide Web and Virtual Reality.* Unpublished. Available from: http://web.mit.edu/comm-forum/mit6/papers/Delgiudice.pdf.

Golbeck, J., Robles C. & Turner K. 2011. Predicting personality with social media. *Conference on Human Factors in Computing Systems* - Proceedings, pp. 253-262

Google. 2013. *Add name tags in Picasa.* Available from:
https://support.google.com/picasa/answer/156272?hl=en [Accessed 04-12-2013].

Gross, D. 2012. Instagram backtracks after user privacy revolt [Online]. *CNN.com*. Available from: http://edition.cnn.com/2012/12/18/tech/social-media/instagram-terms-users [Accessed 19-05-2013].

Hoven, J. Van Den. 2008. Information Technology, Privacy, and the Protection of Personal Data. *IN:* Van den Hoven, J. & Weckert, J. (eds.) *Information technology and moral philosophy*. Cambridge: Cambridge University Press, pp. 301-321.

Ingraham, N. 2013. Apple announces 1 million apps in the App Store, more than 1 billion songs played on iTunes radio [Online]. *The Verge*. Available from: http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store [Accessed 08-04-2014].

Jacquemard, T., Novitzky, R., O'Brolcháin, F., Smeaton, A.F. & Gordijn, B. 2014. Challenges and opportunities of lifelog technologies: a literature review and critical analysis. *Science and Engineering Ethics,* epublication ahead of print.

Johnston, C. 2013. Data brokers won't even tell the government how it uses, sells your data [Online]. *Ars Technica*. Available from: http://arstechnica.com/business/2013/12/data-brokers-wont-even-tell-the-government-how-it-uses-sells-your-data/ [Accessed 23-01-2014].

Kafka, P. 2011. Facebook Brings Back (Part of) Beacon, and No One Blinks. *All Things D.* Available from: http://allthingsd.com/20110126/facebook-brings-back-part-of-beacon-and-no-one-blinks/ [Accessed 19-05-2013].

Kalven, H. Jr. 1966. Privacy in Tort Law--Were Warren and Brandeis Wrong? *Law and Contemporary Problems,* 31(2), pp. 326-341.

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N. & Wetherall, D. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. *Financial Cryptography and Data Security*, 7398, pp 68-79.

Kensington v. Air New Zealand Limited. 2013. NZERA Auckland 384 5421308.

King, M., Hu, F., McHugh, J., Murphy, E., Newman, E., Irving, K. & Smeaton, A.F. 2013. Visibility of Wearable Sensors as measured using Eye Tracking Glasses. *Communications in Computer and Information Science*, 413, pp 23-32.

Koops, E.J. 2011. Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice. *SCRIPTed*, 8(3), 229-256.

Koum, J. 2012. Why we don't sell ads [Online]. *WhatsApp Blog*. Available from: http://blog.whatsapp.com/index.php/2012/06/why-we-dont-sell-ads/?lang=en [Accessed 25-02-2014].

Kravets, D. 2013. NSA Wrongly Says Warrantless Mobile-Phone Location Tracking Is Legal [Online]. *Wired.com*. Available from: http://www.wired.com/threatlevel/2013/12/nsa-cell-site-data/ [Accessed 13-12-2013].

Lessig, L. 1999. *Code: And other laws of cyberspace*. New York: Basic Books.

Lessig, L. 2009. Against Transparency: The perils of openness in government [Online]. *The New Republic.* Available from: http://www.tnr.com/article/books-and-arts/against-transparency?page=0,5 [Accessed 13-02-2012].

Levy, S. 2014. Mark Zuckerberg on Facebook's Future, From Virtual Reality to Anonymity [Online]. *Wired.com.* Available from: http://www.wired.com/?p=802341 [Accessed 13-05-2014].

Locke, J. 1689. *The Second Treatise of Government* (3rd ed.). Oxford: Blackwell.

Margaris, C. 2012. Facebook's New Advertising Method Stirs Controversy [Online]. *The Bottom Line.* Available from: http://thebottomline.as.ucsb.edu/2012/03/facebook%E2%80%99s-new-advertising-method-stirs-controversy [Accessed 19-05-2013].

Mayer-Schönberger, V. 2009. Delete: The Virtue of Forgetting in the Digital Age. Princeton & Oxford: Princeton University Press.

McMillan, R. 2013. Cloud Computing Snafu Shares Private Data Between Users [Online] *Wired.com*. Available from: http://www.wired.com/wiredenterprise/2013/04/digitalocean/ [Accessed 25-05-2013].

Mehdizadeh, S. 2010. Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook . *Cyberpsychology, behavior and social networking*., 13(4), pp. 357-364.

Memoto. 2013. *Weekly update: Improved yield results and software crunch time*. Available from: http://blog.memoto.com/2013/08/weekly-update-12/?utm_source=The+Memoto+Newsletter&utm_campaign=9624e09eca-Newsletter_Issue_105_15_2013&utm_medium=email&utm_term=0_2fa824b0f7-9624e09eca-79596181 [Accessed 04-09-2013].

Meyer, D. 2012. No, what Instagram just did to its users is not acceptable [Online]. *ZDNet*. Available from: http://www.zdnet.com/no-what-instagram-just-did-to-its-users-is-not-acceptable-7000008949/?s_cid=e505 Accessed 19-05-2013.

Microsoft. 2014. MyLifeBits [Online]. *Microsoft Research.* Available from: http://research.microsoft.com/en-us/projects/mylifebits/ [Accessed 19-05-2014].

Mill, J.S. 1859. *On Liberty*. London: Penguin.

Moor, J. H. 1990. The Ethics of Privacy Protection. *Library Trends*, 39(1&2), pp. 69-82.

Moor, J.H. 1997. Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, 27(3), 27-32.

Moore, B. 1984. *Privacy: studies in social and cultural history*. Armonk: M.E. Sharpe, Inc.Moore, G.E. 1965. Cramming More Components onto Integrated Circuits. *Electronics*, 38(8), pp. 114–117.

Murata, K. 2011. The right to forget/be forgotten. In: *CEPE 2011: Crossing Boundaries*.

Nack, F. 2005. You Must Remember This. *IEEE Multimedia*, 12(1), pp. 4-7.

Nakazibwe, C. 2012. Sex Talk: So, who 'ssengas' the men? [Online]. *The Observer*. Available from: http://www.observer.ug/index.php?option=com_content&view=article&id=20749&catid=69&Itemid=104 [Accessed 14-01-2014].

Narayanan, A. & Shmatikov, V. De-anonymizing Social Networks. *IN: Security and Privacy, 2009 30th IEEE Symposium*, pp.173,187.

Nissenbaum, H. 1998. Protecting Privacy in an Information Age: The Problem of Privacy in Public *Law and Philosophy*, 17(5-6), pp 559-596.

Nissenbaum, H. 2004a. Privacy as Contextual Integrity. *Washington Law Review*, 79(1), pp. 101-139.

Nissenbaum, H. 2004b. Toward an Approach to Privacy in Public: Challenges of Information Technology, *Ethics & Behavior*, 7(3), pp. 207-219.

Nissenbaum, H. 2011. A Contextual Approach to Privacy Online. *Daedalus*, 140 (4), pp. 32-48.

Nussbaum, M.C. 2007. *Frontiers of Justice*. London & Cambridge: Harvard University Press.

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

O'Hara, Kieron. 2012. The Technology of Collective Memory and the Normativity of Truth. In: Goldberg, D., McCarthy, N. & Michelfelder, D. (eds.) *Philosophy and Engineering: Reflections on Practice, Principles and Process*, Berlin: Springer-Verlag.

Ohm, P. 2009. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization *UCLA Law Review*, 57(9-12), pp. 1701-1777, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: http://ssrn.com/abstract=1450006

Persson, M. 2014. Dwangsom dreigt voor privacyschending WhatsApp [Online]. *De Volkskrant*. Available from: http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3603163/2014/02/25/Dwangsom-dreigt-voor-privacyschending-WhatsApp.dhtml [Accessed 25-02-2014].

Protalinski, E. 2012. Facebook Likes don't always mean brand loyalty [Online]. *ZDNet.* Available from: http://www.zdnet.com/blog/facebook/facebook-likes-dont-always-mean-brand-loyalty/8885 [Accessed 20-05-2013].

Rawassizadeh, R. 2011. Towards sharing life-log information with society. *Behaviour & Information Technology*, pp. 1-11.

Reiman, J.H. 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, 11(1), pp. 27-44.

Rieger, G., & Savin-Williams, R. C. 2012. The eyes have it: Sex and sexual orientation differences in pupil dilation patterns. *PloS One*, 7(8), e40256.

Rushe, D. 2013. Microsoft and Yahoo! voice alarm over NSA's assault on Internet encryption [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/2013/sep/06/yahoo-nsa-gchq-decryption-abuse [Accessed 09-09-2013].

Sanger, D.E. & Shanker, T. 2014. N.S.A. Devises Radio Pathway Into Computers [Online]. *The New York Times.* Available from: http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-Internet.html?_r=1 [Accessed 14-01-2014].

Scanlon, T. 1975. Thomson on Privacy. *Philosophy and Public Affairs*, 4(4), pp. 315-322.

Schacter, D.L. 2001. *The Seven Sins of Memory: How the Mind Forgets and Remembers*. Boston & New York: Houghton Mifflin Company.

Sengupta, S. 2012. On Facebook, 'Likes' Become Ads [Online]. *The New York Times.* Available from: http://www.nytimes.com/2012/06/01/technology/so-much-for-sharing-his-like.html?pagewanted=all [Accessed 09-09-2013].

Shachtman, N. & Beckhusen, R. 2013. 11 Body Parts Defense Researchers Will Use to Track You [Online] *Wired.com*. Available from: http://www.wired.com/dangerroom/2013/01/biometrics/?pid=1775&viewall=true [Accessed 25-01-2013].

Singer, N. 2013. A Data Broker Offers a Peek Behind the Curtain [Online]. *The New York Times.* Available from: http://www.nytimes.com/2013/09/01/business/a-data-broker-offers-a-peek-behind-the-curtain.html?pagewanted=1 [Accessed 09-09-2013].

Smith, D. 2013. Instagram Loses Half Its Daily Users In A Month, And Here's Why [REPORT]. *IBTimes.com*. Available from: http://www.ibtimes.com/instagram-loses-half-its-daily-users-month-heres-why-report-1014214 [Accessed 20-05-2013].

Sonvilla-Weiss, S. 2008. *(IN)VISIBLE: Learning to Act in the Metaverse*. Vienna: Springer.

Spiegel. 2013. *'Follow the Money': NSA Spies on International Payments* [Online]. Available from: http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html [Accessed 07-03-2014].

Story, L. 2007. Coke Is Holding Off on Sipping Facebook's Beacon [Online]. *The New York Times*. Available from: http://bits.blogs.nytimes.com/2007/11/30/coke-is-holding-off-on-sipping-facebooks-beacon/?_r=0 [Accessed 03-12-2013].

Swarns, R.L. 2004. Senator? Terrorist? A Watch List Stops Kennedy at Airport [Online]. *The New York Times*. Available from: http://www.nytimes.com/2004/08/20/national/20flight.html [Accessed 15-06-2013].

Sweeney, L. 2000. Simple Demographics Often Identify People Uniquely. *Carnegie Mellon University, Data Privacy,* No. 3.

Tavani, H.T. 2000. Privacy and the Internet. *Ethics & Technology Conference June 5, 1999*.

Tavani, H.T. & Moor, J.H. 2001. Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society,* 31(1), pp. 6-11.

Tavani, H.T. 2004. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. Hoboken: John Wiley & Sons Inc.

Tavani, H.T. 2007. Philosophical theories of privacy: implications for an adequate online privacy policy. *Metaphilosophy,* 38(1), pp. 1-22.

Tavani, H.T. 2008. Floridi's ontological theory of informational privacy: Some implications and challenges. *Ethics and Information Technology,* 1, pp. 155-166.

TED. 2011. *Hasan Elahi: FBI, here I am!* [Online]. Available from: http://www.ted.com/talks/hasan_elahi.html [Accessed 23-05-2012].

Thomson, J.J. 1975. The Right to Privacy. *Philosophy and Public Affairs*, 4(4), pp. 295–314.

Time Magazine. 1955. Art: The Oldest Madonna [Online]. Available from: http://content.time.com/time/magazine/article/0,9171,866375,00.html [Accessed 14-01-2014].

Tseng, P.H., Cameron, I.G., Pari, G., Reynolds, J.N., Munoz, D.P. & Itti, L. 2013. High-throughput classification of clinical populations from natural viewing eye movements. *J Neurol*, 260(1), pp. 275-284.

Warren, S. D. & Brandeis, L. D. 1890. The right to privacy. *Harvard Law Review*, 4(5), pp. 193-220.

Weiser, M. 1991. The Computer for the 21st Century. *Scientific American*, 265, pp. 94 – 104.

Westin, A.F. 1966. Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy. *Columbia Law Review,* 66(6), pp. 1003-1050.

5 Autonomy

Introduction

As was the case with privacy, autonomy lacks a clear-cut, ready-to-use definition. The first part of this chapter will address the concept of 'autonomy'. In the second part of this chapter, the ways in which lifelogs influence the *deliberative autonomy* of the lifelogger and others recorded are explained. As lifelogs might improve as well as weaken some of the conditions necessary for autonomous decision-making, the challenges that arise in relation to autonomy are discussed first and then elements of lifelogs that are beneficial to autonomy are discussed. In the third part of this chapter, the ethical challenges for *executory autonomy* are examined followed by an exploration of the ethical opportunities. This chapter is concluded with some recommendations to meet the challenges and realise the opportunities.

5.1   Respect for autonomy

Autonomy is composed of the Greek words '*autos*', which means 'self', and '*nomos*', which means 'law' and was originally applied to describe the political situation of Greek-city states. If a city state could impose its own laws free from the interference by external powers it had *autonomia* (Dworkin 1976). The combination of these two words are a close approximation to the most general meaning of autonomy, namely to be a law to oneself. Now *autonomia* is also applied to individuals. The idea that one should govern oneself can be considered a product of the Enlightenment (Christman 2009). Autonomous agents are competent to reflect on the life they want to live and are capable of pursuing that life. They act on motives, preferences and thoughts which are their own and which are not merely externally imposed. Autonomy has become an influential moral value in recent Western thinking. It has featured both in a wide spectrum of area of philosophy ranging from bioethics to political philosophy. Two accounts have proven especially influential to recent interpretations of autonomy, which will be explained briefly below without claiming to explain their accounts exhaustively.

Kant provides one of the most well-known accounts of autonomy (Kant 1785, 2003 and 2009). Kant's conception of autonomy is obedience to self-imposed moral law (Kant 1785). These moral laws are determined by oneself through reason rather than enforced by clerics or politicians. Causes that do not originate from reason, such as those that are dictated by one's environment and one's desires and inclinations, are inimical to autonomy. Moreover, the capacity for moral autonomous reasoning is a decisive factor for the respect

others owe one and one owes others according to Kant. Because a person, as a rational human being, is capable of imposing moral laws on herself and therefore acts autonomously, she is worthy of respect (Kant 1785). As stated by Kant, one ought not to use other autonomous agents merely as a means to an end, namely using them for one's own goals without considering theirs. Moral autonomy shows similarities to conceptions of political freedom in which the citizens are only free when they are subject to laws of their own making (Johnson 2008). When a country has autonomy, their laws are not externally imposed, but by the people within the nation, and these laws reflect their 'will' instead of that of a foreign power. Similarly, autonomy for the individual is an expression of his own will. Autonomous decisions and acts originate from the individual's rational will responding to reason rather than from his emotional attachments or desires. It has to be noted that according to Kant's conception of the 'will', the will is connected to reason whereas in contemporary academic debates on autonomy the 'will' is often seen to be at least partly constituted by desires and emotions and in relation to others (see for example Benson 1991, Govier 1993, or Rössler 2002).

John Stuart Mill provides another thought-provoking account of autonomy although he never mentioned the term 'autonomy' in his work but uses the term 'liberty' instead (Mill 1859). According to Mill autonomy is not solely concerned with morality. The scope of his concept of morality includes all aspects of life. According to Mill, a person should have the liberty to create his own plan of life under the condition that this plan of life does not harm others (Mill 1859). He remarks that "[t]he only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign" (Mill 1859, 18). Mill is a hedonicistic utilitarian, holding that certain pleasures constitute the good and that those pleasures should be maximised. According to Mill, personal autonomy is essential for human happiness and therefore society must promote autonomy. He gives various reasons for this according to Fuchs (2001). The first is that people conduct "experiments of living" (Mill 1859, 105). People have to formulate their own ends, and for this they need a diverse pallet of compelling alternatives from which to choose. Each person has his own set of characteristic preferences, interests and ends, so he cannot simply follow the life plan of other people. Society can give examples of how others have lived their lives and that can be used for oneself. Secondly, a society which aims to maximise welfare, should offer individuals the freedom to actually pursue their

desires (Mill 1859). A society which fails to guarantee the pursuit of autonomously chosen life plans is of little value to the individual. The value of a society depends on the securities in place to actually follow up on one's autonomous decisions. Thirdly, according to Mill one has to develop one's competency to act autonomously: "the free development of individuality is one of the leading essentials of well-being" (Mill 1859, 105). The competency to choose prudentially and maximise satisfaction is developed over time. One needs liberty to develop this capacity through which one can attain pleasure. Hence, autonomy is necessary in the pursuit of happiness.

5.1.1 *Core components of autonomy*

Two aspects of autonomy, without claiming to advance a complete account of autonomy as other conditions may also be required, seem important to assess the effect of lifelogs on autonomy, namely (i) *understanding* and (ii) *being free from controlling influences*. These two conditions can function as the backdrop to which concerns with the autonomy of the lifelogger and non-lifelogger can be discussed.

(i) One needs to have a good understanding of the relevant aspects of a situation. Obviously, this implies possession of correct information including the relevant facts. Consequently, if one purposely informs someone else with incorrect or in any other way inadequate information (through malevolence or negligence), one might be said to fail to respect her autonomy. In addition, understanding requires sufficient physical and mental capacities for deliberation.

(ii) Being free from controlling influences that determine an action means that one should not be forced into making decisions or perform actions. The actions one performs and the beliefs and desires one holds are actually 'willed' by one rather than imposed by others. Freedom is the focal point for this condition. There are several ways in which freedom can be compromised or in which others can influence the person to such a degree that it would not be reasonable to consider her actions to be willed by her or to consider her beliefs to be truly hers.

To respect the autonomy of others then is to recognise that they have a right to hold their own values and beliefs and to allow them to act in accordance with them. Therefore, respect requires more than refraining from interfering or hindering the conditions for autonomous choice, e.g. infringing the freedom of others so that they cannot execute

autonomous decisions. When reasonable it also requires positive actions, e.g. informing others about their situation so that they can make reasoned decisions. For instance, a doctor should not only refrain from deceiving his patient, but should inform the patient truthfully in order to let the patient decide *and* should take into consideration that a patient has his own interests and beliefs.

5.1.2 Executory and deliberative autonomy

The effect of the usage of lifelog technology on the autonomy of lifeloggers and non-lifelogger will be discussed on two levels: deliberation and execution. For both one would need sufficient and adequate information and some freedom from the imposing will of others.

Deliberative autonomy is considered the ability to form authentic desires and beliefs. By 'authentic' it is meant that people are able to reflect on their desires and beliefs from a distance to judge if they consider them as their own rather than the result of oppressive social structures (Rössler 2002). This idea of authenticity is not necessary an atomistic one as a person develops this ability in intersubjective exchanges with others and within power relations. Executory autonomy is the personal freedom to perform actions that are willed by the person so that the person can shape her life according to her authentically held desires and beliefs. Without sufficient information one's executory autonomy can be impaired, e.g. the person may refrain from acting according to her values and beliefs because she thinks she lacks the freedom although she has in fact the freedom. These two levels are distinct. One might have deliberative autonomy and have an authentic desire to do 'X', but lack executory autonomy because one's social environment prevents one from doing 'X'. Similarly, one might not have an authentic desire to do 'Y', but the personal freedom to perform 'Y'. Nonetheless, the degree of autonomy experienced at the level of execution can affect one's autonomy on the level of deliberation and the other way around. For instance, the problem of 'adaptive preferences' may occur. People who structurally cannot achieve a goal could lose their desire for it over time (Kymlicka 2002). Conversely, someone who is indoctrinated to believe 'X' may not make the resources available to do 'Y' as well, effectively impairing her personal freedom to do 'Y'.

Autonomy on both levels is a matter of degree. One's decision can be of greater or lesser autonomy depending on the situation. For ideal autonomy on both levels one would have a complete understanding of all relevant information and be absolutely free from external pressure. This may be impossible. Furthermore, the degree of autonomy can depend

on the situation, e.g. one may be less autonomous concerning smoking while more autonomous deciding on the book that one wants to read next.

5.1.3 Justification for the use of the principle

The importance of autonomy is widely accepted within the contemporary debate to an extent that the principle respect for autonomy hardly needs any justification. There seems little disagreement that autonomy and respect for autonomy are normatively relevant.[79] Respect for autonomy has a place in the three main streams of normative ethics in Western thinking, namely deontology, consequentialism, and virtue ethics. However, the importance of autonomy is not limited to Western thinking (Sen 2001). Moreover autonomy is judged important as it is considered necessary for other values. In this section, four short examples are provided to illustrate the broad acceptance of autonomy as a principle.

1) There is a deontological, Kantian justification for respect for autonomy; because an agent is autonomous, he has dignity and merits moral respect. Kant's justification has implications that conflicts with commonly held moral intuitions; if autonomy would be the sole ground for dignity and respect, people who lack the competence to make autonomous decisions would also have no human dignity and are as a result no recipients of respect. However, typically one would consider people without the competence for autonomous decision-making worthy of human dignity.

2) Mill offered a consequentialist justification for respect for autonomy: autonomy is a key element to well-being. Some consequentialists consider autonomy to be intrinsic to well-being, while others consider it to lead to well-being. Hare shares the latter position from a utilitarian perspective as he states that slavery is wrong and that people need liberty because "the principles which it is best for them to have are those which will lead them to make the highest proportion of right decisions in actual cases where their decisions make a difference to what happens – weighted, of course, for the importance of the case, that is, the amount of differences the decisions make to the resulting good or harm" (Hare 1979, 115). Liberty is such a principle according to him.

3) Dworkin (1976; 1988) and Frankfurt (1971) provide a slightly different justification than the Kantian, namely that autonomy is the ground on which particular

---

[79] Nonetheless there is some criticism about the value attached to autonomy (especially Beauchamp and Childress are criticized for giving autonomy too much weight) (Foster 2009) and some even reject the value of autonomy as desirable altogether (Hoagland 1988).

decisions and actions merit respect. Imagine the act of a smoker who wants to quit but still lights up a cigarette because he is addicted. The act of smoking is not the result of an autonomous decision and so deserves less respect. As a result, one can put some pressure on him to give up this habit without harming his autonomy. His autonomous choice to spend his money on fixing his house rather than buying a new car does merit respect following Dworkin (1976).This justification is more contextualised than that of Kant according to whom one deserved respect on the basis of being an autonomous agent.

4) Autonomy can also be considered valuable within virtue ethics. The ability to govern oneself can be a virtue and a necessary requirement for human flourishing (Piper 2010).

Hence, within normative ethics, autonomy can be important in deontology, consequentialism and virtue ethics.

5.2   Challenges to and opportunities for deliberative autonomy

After this brief discussion about autonomy and respect for autonomy, the assessment of how lifelogs can impair and promote autonomous decision-making can take place.[80] The working definition of a lifelog identifies it as a digital record about an individual's quotidian activities using data which are gathered, stored, and processed into meaningful and retrievable information as a personal digital archive of multimedia data (*2.1 Definition of a lifelog*). From this definition one can conclude that the most general use of a lifelog is that it provides an individual with personal information about his daily activities. The personal information from lifelogs might be used to reflect on one's life and maybe change it. Take for example Saga, one of the first lifelogging programmes for the smart phone, which has as a tagline on its website that reads as follows: "Share your *authentic* life with the people that matter most. … Saga automatically records *your real life story*, as told by the places you visited and the things you've done. … *Capture every moment*, even the little ones, in your lifelog. Learn about your habits and *set meaningful goals* with *the insight you gain"* (Saga 2013: my italics).[81] Behind this hyperbole is revealed an idea that maybe refers to a fundamental

---

[80] Below liberty is discussed, which is the freedom one experiences to execute decisions. The separation between the two might be somewhat deceiving as liberty can influence values and beliefs and vice versa. The separation of autonomy on the level of deliberation and autonomy on the level of execution shows similarities to Berlin's distinction between positive and negative freedom (Berlin 1958).

[81] Autographer has the same kind of texts on their websites: "Autographer takes very different photographs. They are always natural, unexpected and completely authentic. … Now you can re-tell your unique travel story

assumption about the functioning of lifelogs, namely that lifelogs, or technology in general, can offer an immediate and unmediated overview of one's experiences. There is a second and related assumption, namely that this information betters one's understanding of oneself and others. However, as will be discussed below, the first assumption seems unwarranted on closer inspection while the second is only conditionally true.

5.2.1 Challenges to deliberative autonomy

First, the ways in which lifelogs can be unfavourable to deliberative autonomy are discussed. There are five ways explained in which the content of lifelogs might be pose challenges to deliberative autonomy.

5.2.1.1 Biases

The assumption that lifelogs capture reality as such is discussed first.

The assumption that lifelogs capture reality as it appears might seem appealing to some. Suppose you have taken a photo of a situation, for instance, of your family at Christmas, and retrieve that picture to refresh your memory of the situation. The picture does not seem to convey any bias. It seems to present *facts* as they are. You see your parents, grandparents, siblings, their parents, your partner, the dog and a table with food all within one photo and captured by a device which seems indifferent to your interests or needs and seems to have no interests of its own. This photo seems more reliable than your personal or another family member's description of your father's attire and the dessert you made.

Indeed, a camera is unable to have bias in the same way people do. However, this latter point obscures the fact that technology is the result of a process involving people with biases and interests and the fact that technology itself has limitations when capturing information. Even without any intention to mislead or misinform the lifelogger, indeed, even when developers aim to provide an 'objective' account of reality it is impossible to present information devoid of theoretical assumptions and other biases. Below a few of those biases are discussed loosely ranging from very abstract to very concrete.

Axiological bias: There are fundamental issues that render it impossible to capture unmediated experience. According to some philosophers, scientific facts are created within a system which is dependent on values and axioms that are assumed rather than irrefutably

---

as you lived it. And hold onto the memories for a lifetime" http://www.autographer.com/#home , April 23rd 2014)

proven (Putnam 2002; Quine 1963). The fact-value dichotomy, namely that it is possible to obtain facts without using values, is heavily disputed (Putnam 2002). Positivism in the sense that empirical knowledge is the immediate and unmediated reduction of experience is considered untenable by Putnam (2002) and Quine (1963). The sharp dichotomy between facts and axiological values is illusive according to them. Assuming this is true, lifelogs at a very fundamental level cannot capture reality as it is or appears without using presupposed values. Nonetheless, the idea that lifelogs might not offer value-free, unmediated reality seems hardly sufficient reason to dismiss them as a valuable source of information to better one's understanding of one's past choices. Even when lifelogs fail to capture unmediated reality, they might still provide people with useful information. Similarly the findings of science should not be dismissed altogether, even if they would fail to offer a valueless representation of reality. At most this limitation requires those developing and marketing lifelogs to carefully consider the epistemological claims they make and the instructions they provide. Instead of presenting lifelog data as kernels of unmediated and undisputed truth, they could use more moderate language and present their information as findings or estimates. In addition, lifeloggers have to be aware of the limitations of lifelog information.

Technological bias: The technological bias is another bias. Lifelogs convey solely information that can be digitised rather than capturing experiences or reality in its entirety.

There are important elements of one's life that cannot be captured by sensors or algorithms. The fact that lifelogs are an inadequate instrument to capture subjective experience and context has already been discussed in the literature review albeit not in relation with autonomy (Curry 2007; Dib 2012; Van Dijck 2005; Van Dijck 2012; Murata 2011). Also this can be shown by a simple scenario. Suppose you are going to a restaurant to celebrate your grandmother's 80th birthday. Although you love your grandmother, you would rather be spending the Saturday evening at the cup final of an international tournament with your friends. Your unhappiness is aggravated by the fact that you are seated in the corner next to the unpleasant person who is the wife of your uncle. The dinner takes place in a steakhouse that serves average food with little nutritional value and which is quite expensive. Notwithstanding these disadvantages you still feel obliged to go. Often the trade-off between instant gratification and short term benefits for personal, social or ethical considerations, is considered fitting. In the scenario you wanted to be a good grandchild (or, more general, a good person) and are prepared to make this kind of sacrifice at least once a year. This ethical and/or emotional dimension is not a measurable condition of the physical world and therefore

135

cannot be captured by sensors or algorithms. Indeed, the lifelog may annotate this event as undesirable because of its effect on stress-levels, health, and your finances. Non-measurable things such as context, empathy, compassion, ethical considerations have no obvious place within the lifelog but they are of utmost importance when formulating one's goals or understanding one's actions and oneself. Indeed, these are the considerations that are communicated during interpersonal contact. By exclusively or predominantly focusing on lifelogs, other relevant aspects are obscured and as a consequence one's understanding would be impoverished rather than enriched.

Another example is that of written or verbal language. Symbolism in written or verbal language is difficult to capture using algorithms and sensor devices. The fact that some opinions have a more far-reaching symbolic value than just being a desire or belief about the object is sometimes made explicit. For American politicians denying climate is more than solely a statement about scientific facts and methods, it is more value-loaded than one may expect. Denying climate change hurts, for example electoral support of voters under 35 and reflects negatively on the perception of their values and capacity for leadership (Levin & Striple 2013).[82]

There are other reasons that lifelog content will reflect the state of current technology rather than unmediated reality of a more practical nature. Technology is (presently) unable to measure all physical conditions that would be in theory measurable: some conditions cannot be measured even though they are physical. In other cases, one might lack the algorithms to infer conclusions. As a consequence, the content of lifelogs is a reflection of technological possibilities. Moreover, sensor technology or algorithms are subject to systematic or random errors. As a consequence, lifelogs can approximate the conditions they are intended to capture but will not be an exact representation of reality.

These limitations do not preclude lifeloggers obtaining a greater understanding about events when using lifelogs. For some information, lifelogs will be more accurate, such as information about the physical appearance of the clothes one's father wore or the date one went for lunch in a particular place. Also, a lifelog may provide the lifelogger with more accurate information than she would have had without it, such as information about exercise, carbon footprint, or health. Indeed, the technological bias does not preclude autonomous

---

[82] Even 47% of voters under 35 that are Republican, consider it less likely that they would vote for a climate change denier according to Levin and Striple (2013).

choice but again requires the developers and lifeloggers to show some reticence when presenting or applying lifelog data.

Stakeholders' bias: Also stakeholders influence the information that is made available through lifelog technology. The idea that there are social processes that influence the design and use of technology is not a novel one and has been identified with relation to technology other than lifelogs (Bijker, Pinch & Hughes 1987; MacKenzie & Wajcman 1999). There are many stakeholders involved in the process of designing, marketing, and consumption of lifelogs that could exert some influence on the design, use and marketing of the lifelogs. As a consequence, the marketing, design, and use of lifelogs will be a compromise between different interests, such as: legal regulations and limitations; technological feasibility; aesthetics; user-friendliness; ethical considerations; consumer interests; economic viability; social acceptability; *et cetera*.

There is a lot of variation possible regarding the design of lifelogs, such as the devices used, the data gathered, the information made retrievable. Out of the previously mentioned interests, social acceptability, for one, is a factor with a cultural component that might affect the functioning and usage of lifelogs. Lifelogs that are ill-fitted to the standard of decency of their target market are unlikely to succeed commercially. Standards of decency, however, can vary greatly between individuals and cultures. Sometimes opposing views are revealed when a corporation wants to enforce their standard of decency too stringently. The technology giant Apple, for instance, stirred controversy when censoring an application that contained depictions of homosexual acts or of 'gay culture' for reasons of obscenity and pornography, even though applications showing similar images of heterosexual intimacy were allowed (Tate 2010a; Tate 2010b). Another technology giant, namely Facebook, has had similar issues when censoring photos of women breastfeeding their babies.[83] Most likely as a result

---

[83] According to Facebook, only photos which other members on Facebook reported as offensive were removed after they were being checked. In the case of a photo being removed, while not being too revealing according to the policy, Facebook blamed it on incidental mistakes made by employees. This statement can be doubted as the same kind of pictures from the same woman was removed twice which sheds doubt on the assertion that it is incidental (Matyszczyk 2013; Protalinski 2012). However, after the popular outcry on the subject, Facebook seems very aware of the issue. Currently the standard is as follows: "Photos that show a fully exposed breast where the child is not actively engaged in nursing do violate the Facebook Terms. These policies are based on the same standards which apply to television and print media" (Facebook 2013a). In the section on what content is removed it reads: "Facebook has a strict policy against the sharing of pornographic content and any explicitly sexual content where a minor is involved. We also impose limitations on the display of nudity. We aspire to respect people's right to share content of personal importance, whether those are photos of a sculpture like Michelangelo's David or family photos of a child breastfeeding" (Facebook 2013b). However at other times they

of the popular outcry resulting from censoring photos of mothers breastfeeding, Facebook relaxed its policy, which, again, is a sign how different stakeholders, in this case consumers, can influence information retrieval on particular platforms. It will be difficult for lifelog companies to distinguish whether data are appropriate, while not advancing too narrowly a concept of right or good.[84]

Moreover issues may arise when semantic meaning is attached to data to improve information retrieval. The taxonomy used for matters such as gender or sexuality might fail to recognise the complexity of contemporary society. Lifelogs might present gender as a binary option, male and female, while some people may consider themselves neither one of them. By doing so lifelogs might involuntarily or indirectly promote a limited conception of reality. Facebook acknowledged this issue by offering 50 different choices for gender (which are currently only available to members in the US using the English version) (Ball 2014). For lifelogs, these issues might be ingrained in the algorithms that organises information, e.g. to identify a woman algorithms must be able to identify typical feminine behaviour or appearance and consequently have an tacit understanding of what constitutes as typically female behaviour or what is considered to be typically female behaviour. Some lifelogs might use specific algorithms that adjust on the basis of what other lifeloggers have requested and by doing so they effectively promote the taste of the general public.

In a way a technology will always be the product of social processes. Again these issues with biases are not decisive as biases can occur in any medium, but they should be scrutinised in order to see if they fit the people and events that they are supposed to describe.

Cultural bias: A 'culture' is here considered to be a particular group of people sharing a set of beliefs, values, customs and behaviours. Objects, events, forms, styles, ideas, symbols, sounds, and classifications can have their own idiosyncratic meaning within these communities. To design lifelogs that detect events, some familiarity with traditions and

---

have stated that photos that showing the areola is the decisive factor in deciding the appropriateness of the photo. The societal rejection of breast feeding could lead to women refraining from doing it while it has advantages to the baby (Gerster Trocola 2005). Similarly to previous privacy concerns, with lifelogs mother may refrain from doing so because they would not want to be captured on camera either showing accidentally too much skin or breast feeding in public. Corporations reinforcing that behaviour by judging photos with too much skin inappropriate may only confirm current tendencies.

[84] Although some search queries might be considered morally reprehensible, the information may be innocuous in many other circumstances. Photos of your young children swimming in a pool naked can be innocuous and emotionally valuable. However, if these photos are searched with the sole intention to see them to satisfy one's lust the retrieval of this information seems undesirable.

cultural conceptions of events is necessary. The significance and importance of traditions, such as Christmas, Eid al-Fitr, and Valentine's Day, depend on culture and the ability to search for these events are more likely to be found in lifelogs that are developed by people who are aware of them. The mere existence of specific information implies that this information is or can be relevant to lifeloggers. To strive for a particular weight, to spend sufficient time with the children, or to eat organic food, is more significant to some cultures or groups than others.[85] Even, the lay-out of the user-interface using culturally specific signs such as colour and placement to indicate to the user what is most interesting can be culturally determined. In Western countries people read from left-to-right and from top-to-bottom. Consequently, designers will likely follow these rules when developing interfaces for Western Markets. Instead of lifelogs providing unbiased and value-neutral, they might be a vehicle to promote specific cultural traditions and customs.

Lifelogs do not necessarily have to reflect a particular cultural conception. For example, lifelogs could just as easily convey non-Western as well as Western values as they will likely reflect the culture in which they are used, or, more specifically, the target group by which they are used. A lifelog would lack popular support if there is an insufficient fit with the culture in the market that it is sold.[86] After all, the presence of Asia based technological companies and the increased political and economic power of Non-Western countries could influence the workings of the technology. Indeed to fully exploit the functionalities of lifelogs the lifelogger needs to appropriate or at least have a minimal understanding of the beliefs and values of developers that led to the current shape and form of the lifelogs and the content that is being presented and retrieved. In other words, lifeloggers need to understand why particular information is presented to them and why the company chose this way of presenting information, e.g. the colours used for information feedback, reading directions, the usefulness of having information about calories, *et cetera*. In turn to do so developers should present information in a way that is comprehensible for prospective lifeloggers. By doing so, both existing cultural values and beliefs and the beliefs and values of developers become affirmed and more firmly solidified. These values become even more explicit when lifelog applications provide advice or otherwise encourage particular behaviour such as tips to

---

[85] The ideal weight has a cultural component as thinness can have different connotations. While some cultures may consider thinness aesthetically and physically ideal, in others curviness is preferred and thinness represents poverty and sometimes even diseases such HIV/AIDS.

[86] The lifelogs would show large similarities cross-cultural but their use, adoption and maybe design might vary, which is also the case with for example smartphones (IAB & IIAC 2013).

achieve a particular weight, spend more time or eat organic food. Conversely even the information that is left out or censored from the lifelog can reveal bias. A failure to bestow certain distinctions could imply that this information is irrelevant or inappropriate.

Some might argue that cultural diversity is necessary for autonomy and that one should therefore forbid cultural outings that could jeopardise diversity.[87] Currently products, brands, and cultural expressions, such as movies, books, political systems, music, and food, all of which arguably have had and still have a great impact on culture and possibly more than lifelogs will ever have, are allowed to proliferate. Indeed, in many cases corporations are embraced that offer products and services that have a disruptive effect on the existing culture. There seems no apparent reason why a possible bias within lifelogs is more harmful than the ubiquity of values in other cultural products and practices currently widely available. A more fundamental concern is that forbidding cultural outings because they are foreign may open the door for far greater hindrances to deliberative autonomy than lifelogs would pose, as this kind of censorship would require some sort of system to decide which cultural product is suitable for the general public and which need to be forbidden. Censoring cultural outings based on their foreignness could lead to greater infringements of autonomy as many different cultural expressions would be subject to scrutiny, e.g. a decision has to be made if a particular movie, piece of music, or literary work is permissible. Indeed, autonomy seems to entail that people should be able to experiment with customs and traditions from other cultures rather than to have their existing culture stringently enforced. In addition, outlawing particular cultural outings that are considered foreign misinterprets a culture as a static entity that is not subject to change. Maybe protecting a culture demands a positive approach of identifying and stimulating practices that are deemed one way or another as valuable to be preserved in some capacity or another rather than a negative approach of forbidding foreign cultural outings such as lifelogs.

Developer's bias: The choice of the developers accounts for another bias. There are other practical limitations that render it unlikely that every aspect of the physical that can be captured *will* be captured at all times. Developers have to choose which sensors and algorithms to include or exclude as it is unattainable for them to incorporate all possible

---

[87] One could argue that cultural diversity is valuable in and of itself and that lifelogs jeopardize cultural diversity but this would an argument that is not based on autonomy. According to that argument one would make autonomy subordinate to cultural diversity rather than to protect autonomy.

sensors or algorithms.[88] Developers are able to select from a diverse range of sensor devices and algorithms that will slightly measure conditions differently. The choice between components of a photo camera has an impact on the content of the photos. By using a camera which focuses on objects in its proximity, one obtains less information about the environment further away. Similarly, by carrying a photo camera around the neck, a different point of view and different things are captured, than when the camera is built into the lifelogger's glasses. The choice which is the most adequate and appropriate representation is one which is made by the developers.

The choices of developers will have considerable consequences for how the lives of lifeloggers will be presented to them within the lifelog and even in what terms and concepts their past will be presented to them. In order to improve the functioning of lifelog technology the augmentation of data with semantic meaning is likely to be required. It would greatly support the retrieval of information if the lifelogger could search for concepts such as 'birthday', 'ill', or 'snorkelling'. The attachment of semantic meaning could negatively affect the lifelogger's understanding if the chosen concepts are poorly defined: for example in the scenario in which Paula wanted to retrieve information about the time spent with her children (*2.5 Scenario*). To attach semantic meaning to data, developers need an idea of what 'spending time together' entails. This is by no means clear-cut or well defined. These interpretations can be culturally determined and fuzzy: does communicating with her children through ICT, such as the use of video calls, count as "spending time together"? If spending time together means physical proximity, would only physical presence be sufficient? It is possible to be in the same room while sleeping on the couch, reading the newspaper, serving customers or watching television or will these activities need to be discounted?

Sometimes these biases will confirm or strengthen existing prejudices and power relations. Masculine concepts and ideas could be overrepresented which would lead to people's life being defined (and maybe judged) based on male standards supporting a male-dominated culture privileging the lifestyle of men. With the low number of women in technology, this is a relevant concern (Marwick 2013). An example of such a perceived masculine bias can be found in some of the applications on one's smartphone that quantify sexual activities such as the application 'Spreadsheet'.[89] This application provides an

---

[88] Practical reasons could be amongst others the wearability, simplicity or reliability or economic viability of the device. Other reasons are of course the previous cultural and personal choices on appropriateness.

[89] More information can be found at: http://spreadsheetsapp.com/

overview of 'thrusts', 'duration', and 'decibel peak' implying that these are the relevant variables to measure intimate acts. It promotes a very limited conception of sexual activity, which is of doubtful benefit in any other way than as amusement. Taken seriously, it would obscure what is important by rewarding behaviour that fails to capture that which is truly significant. By doing so, it facilitates not only a skewed understanding but also implicitly seems to promote a heterosexual, male-biased conception of sexual activity. By designing lifelogs carefully undesirable biases that promote undesirable power relations could be prevented.

Conclusion: The information lifelogs contain is not an immediate representation of reality but is the result of personal, social, moral, legal, and technological limitations and interests.

Lifelogs can affect one's memory and perception which seem intimately related to how one perceives oneself and one's environment (Clowes 2012; Dib 2008; Moreno 2004; O'Hara 2010b). As mentioned in the literature review, memories are dissimilar to data, as they are subjective revisions of the past rather than an unchanging set of data. In contrast to a photo which is taken once at a certain point in time, a memory is constructed whenever it is prompted. This process differs each time; hence the memory changes (Del Giudice & Gardner 2009). Lifelog information will influence the process of memory retrieval by cueing memories. Because memories are malleable, a lifelog can determine to a great extent how lifeloggers come to view and assess an event and ultimately themselves and others. If lifeloggers would solely reflect on themselves using lifelog information, lifelogs would impoverish their understanding of their past rather than augment it.

One might argue that lifelogs are likely to be one source amongst many so that one could consult other information sources: the lifelogger might have other news sources that prevent the lifelog from becoming too dominant. However, for some information lifelog technology would be the sole source of information and for some purposes one might only use lifelog technology, regardless of whether that would be appropriate or not. In addition, these issues become more worrisome when the corporations owning the lifelog services or products also possess control over other media. Major companies such as Google, Facebook, Microsoft, Apple, and Amazon seem to attempt to position themselves as gatekeepers to information. A way of limiting the power of companies is to ensure that no one company

becomes too dominant. One could doubt if one single company should have access to people's lifelog data while also being the gatekeepers to news or the web.

Issues with bias are insoluble and decisive if one demands lifelogs to present value-neutral information. However, one does not (and cannot) require information to be devoid of value as no sources of information would fulfil this standard; one would be left without any sources of information. Despite their limitations many sources of information do in fact increase one's knowledge of events, oneself, or others. Nonetheless it is important to acknowledge the possibility of bias and related limitations to lifelog information. Even though information cannot be entirely devoid of bias, attempts can be made to minimise or reduce those biases that seem inappropriate or undesirable, such as biases that promote behaviour that harm lifeloggers and non-lifeloggers.[90] For example, the aforementioned bias towards masculine concepts might be avoided by carefully designing the lifelog. An advantage of lifelogs is that they can make existing biases more explicit. The information contained in the application Spreadsheet or the censorships of employees of Facebook made these existing biases more visible. These biases may be more easily discussed when they are formulated than when they are implicitly available.

Acknowledging the possibility of bias has another advantage, namely it could prevent lifeloggers from excessively relying on lifelogs. Due to the accuracy and the comprehensiveness of lifelog information, lifeloggers might fail to comprehend the limitations of it. Correct usage will require intellectual and emotional strength as lifeloggers need to distance themselves from information directly related to their lives and select only the information they consider fitting to their purposes. Developers could anticipate misuse, namely by showing that lifelog information is somewhat limited. Suppose a photo-album provides the viewer with the sole tangible token of an event. These albums are often considered useful and sometimes important. Their importance can be explained because they are considered quite limited in the information they convey. They offer the viewer sufficient space for interpretation. Strictly speaking a lifelog does not exclude space for interpretation although the vastness, accuracy, and comprehensiveness, can sway the lifelogger into believing she does not require additional information. Therefore, to design a lifelog so that it leaves space for interpretation would be desirable, for example: by offering the user the

---

[90] In the chapter on beneficence (*6.1.2 Value*), a list of things of intrinsic worth is mentioned. One could consider biases that harm these undesirable.

feature to manually correct measurements, the option to add data sources and annotations. The implicit message is that information is limited and possibly faulty.

Issues with bias do not render the technology necessarily ethically undesirable, but they are evidence that lifelogs should be developed, marketed, and used prudentially, if at all. It is questionable if this challenge will, in fact, be addressed: the prudential development of lifelog technology may require additional investments in time and resources that a company in a highly competitive market and, quite possible, little starting capital may lack. Expertise may be required and features and structures need to be developed so that bias can be avoided or addressed, which can be both financially expensive and time-consuming. Furthermore, these kinds of issues highlight the need for further discussions on existing biases both in design as well as in society in general.

5.2.1.2 Persuasion/Manipulation

Persuasion and manipulation are different from the above mentioned biases as information is now actually purposely altered to skew the judgements of lifeloggers. There might be commercial, political or other interests in play. The internal functioning, the retrieval, the content as well as the presentation of content can be altered to influence the understanding of the lifelogger.

1) Persuasion is to steer someone else's beliefs and desires and can be ethically sound (Beauchamp & Childress 2009, 133). It is not necessarily unethical to persuade the lifelogger to eat healthier or exercise more. When persuading people one can appeal both to their rational and emotional capacities. The issue with persuasion is that it can be directed to invoke emotions, which obscures one's best interests or authentic desires. For instance, corporations may pay to influence the retrieval of information. They could use the lifelog as a platform for advertisement. When searching for an event in a lifelog containing photos from a wearable camera one is likely to be presented with only a few representative photos of the event so one does not have to browse through a whole collection of unfiltered photos. Advertisement companies might pay to bias the lifelog in retrieving photos containing their logo or product.[91] As a result, the lifelogger might retrieve information of events featuring a

---

[91] Under certain circumstances this might be allowed provided that the information retrieved is a fair depiction of the state of affairs and the information is not changed for commercial purposes. Especially when lifelogs are a service that is free of charge, the lifeloggers should expect to have to exchange something. Similarly to Google, Twitter and Facebook presenting advertisements, lifelogs should reveal that a specific search results is retrieved

Coca-Cola bottle somewhere on the fore- or background for the sake of the company rather than the interest of the user. This is a kind of 'product placement' similar to what is currently already present in movies and books (Rich 2006; Guardian 2013). Only this time it is your lifelog data that function as the background to promote these products.[92]

Also third parties could pay to allow certain information to feature more prominently. They can stress certain aspects. For example, pharmaceutical companies can request certain health patterns to be highlighted in the hope that lifelogger will proactively purchase their products. A corporation which produces vitamin supplements may pay to have information about a lack of exposure to sun and deficiencies in nutrition prominently featured to boost its sale of vitamin D supplements. Another way to persuade lifeloggers is to influence the valuations of events. For example, multinational food and beverage companies can pay the lifelog company to incorporate ideas about health that are favourable to their products. To do so, they do not necessarily have to deceive the lifelogger or merely use them as a means to their end. Sometimes scientific consensus is lacking or science offers space for interpretation, for example the specifics of what constitutes a healthy diet provide some room for interpretation and a general consensus seems lacking. Companies can use the room for interpretation in their favour so that lifelog promote products and services based on findings in the favour of a corporation.

Moreover the personal information about the lifelogger contained in a lifelog can be used to persuade the lifelogger with customised advertisements. Lifelog companies might not only have access to data that can reveal much about the lifelogger but can also possibly see if the lifelogger actually responds to their marketing. Corporations might obtain an incredible way to influence the lifelogger as they can tweak the functioning of the lifelog device and application to obtain the best results for them or indeed the advertisements and marketing outside the lifelog. For example, companies can change their physical appearance of their shop or their products based on lifelog information. Another opportunity would be to target people that find themselves in a particular situation. Personal information can give companies an enormous influence over other people's choices.

---

for commercial purposes. Moreover, it should be made clear that some companies might have invested in the development of the lifelog.

[92] These promotions can be offered without providing advertising parties access to this information. Lifelog companies can change algorithms to affect retrieval. This diminishes privacy concerns to some extent.

An additional concern is that it may be unclear to the lifelogger if other parties have vested interests in altering lifelog content. There are cases known in which the retrieval of information was manipulated for financial gain. US Internet providers redirected search queries to an online marketing company that in turn directed it to retail websites (Giles 2011) although the legality of doing so might have been questionable.

These interventions are not necessarily unethical, namely: if the information offered is trustworthy and useful, does not harm the interests of the lifelogger or non-lifeloggers, and the lifelogger is informed about the intervention, then these interventions do not have to be unethical.[93]

2) Manipulation is understood as (successful) attempts to deceive people into behaviour desired by the manipulator indifferent to the interests of those manipulated and is antithetical to autonomy. This is a more nefarious use of lifelogs than persuasion. In the context of lifelogs manipulation entails the covert alteration, distortion or withholding of information to misrepresent the situation without regard for the lifelogger. In contrast to persuasion in which the information presented was truthful this could actually affect the reliability of the content. There are various ways in which the gathering and processing of data can be tampered with. For instance, developers could do so by setting the default to over- or under- 'log', i.e. to design the system so that the default margin of error is set to either over- or underestimate the condition. If corporations want to sell vitamin supplements, they may pay to have the intake of vitamin 'under-logged'. There are other ways to manipulate content. Slight alterations have proven to be profitable under certain conditions to sell products. Yoshida et al. (2013) showed that manipulating one's facial expression in real-time in a mirror makes one more likely to purchase a product. A recent experiment on Facebook showed that by manipulating the algorithms that determine the content which is offered to users on their news feed, the users' emotional states could be affected (Kramer, Guillory & Hancock 2014). Two parallel experiments were conducted for this research: there was a reduction of (a) the positive content or (b) the negative content to which people were exposed. The results showed some correlation indicating emotional contagion, although the

---

[93] Sometimes these advertisements are unethical as they promote a product that can harm the interest of a person; they can negatively affect health or finance or the lifelogger is not informed that the lifelog is used for these purposes.

effect was small.[94] Lifeloggers are especially vulnerable when the information provided cannot be checked by the lifelogger. Feedback about stress levels or heart rate or other information about things that one is unable to sense or ways in which information retrieval is manipulated are often hard to control enabling a greater window for distortions of reality.

Ill-protected lifelogs leave lifeloggers vulnerable to other parties as well. Various kinds of third parties can have an incentive to manipulate lifelog information to influence the behaviour of the lifelogger ranging from corporations to authorities and from religious movements to criminal organisations. Currently, the societal value that is attached to lifelog information and to what extent society permits one to question their output is uncertain. If lifelogs capture information more precisely in many cases, it is likely that the use of lifelog information will be encouraged over the lifelogger's judgements in some situations.[95] Societal pressure to appropriate the results of the lifelog would leave lifeloggers vulnerable to manipulation. However, it also implies that the lifelog would often be reliable. If trust in lifelogs is structurally undermined by parties trying to manipulate lifeloggers then it seems unlikely that lifelogs will become an established source of reliable information. Similarly to a news source that needs to maintain some measure of accuracy to be considered reliable, a lifelog cannot structurally deceive the lifelogger without losing its persuasive powers. Hence, the scope for manipulation is somewhat reduced.

Conclusion: Lifelogs leave the lifelogger vulnerable to manipulation and persuasion. A lifelogger's past within the lifelog might, in the most literal sense, be defined by third party interests that are out of sync or indifferent to his interests. To protect the lifelogger's autonomy, unethical persuasion and manipulation should be avoided. Instead, the lifelog company should provide the information that is first and foremost considered to be in the lifeloggers' interest in obtaining more information about their past rather than primarily serve the interests of other parties. Another recommendation to address this issue is to prevent third parties from manipulating content or information retrieval. The lifelog should be secured against third parties attempting to access data and algorithms.

In addition, the purposes to which personal data are used need to be explained, as users may be unaware that their lifelog promoted a certain consumption pattern or a certain state of mind rather than just provide them with the best possible information about their past.

---

[94] Interestingly, this research also showed indication that accessing positive posts by friends do not seem to affect people negatively through social comparisons.

[95] Further thoughts on this can be found at in chapter 7.2.3.4 Embedding in society.

Under some conditions lifelog retrieval may be altered to suit the purposes of third parties, such as companies, but only when the lifelog provides a truthful account that primarily serves the interest of the lifelogger to be informed about his past, the interests promoted do not harm him or others, and he is informed about the intervention. It is to be expected that some companies may not do so, because sometimes these forms of persuasion or manipulation can be more effective and commercially successful if not explained to the users. Also, explanations of commercial or other interests may deter potential consumers and current users from using the technology undermining the want of a company to explain its choices.

5.2.1.3   Overload of information
There are other reasons why lifelogs could hinder one's understanding of oneself or one's environment. One of them is that by providing lifeloggers with even more information, it becomes even harder for them to make decisions. This argument can take different forms.

1) The first is that lifelogs offer more information to a society which is already swamped with information. This issue has already been discussed in the academic debate on the ethics of lifelogs. O'Hara (2010a) elucidates this concern by referring to Funes the Memorious - the main character in a story of Jorge Luis Borges (1962). Funes obtained a memory that could be said to function as a lifelog. His memory had become effortless infallible, and continuous after he suffered an accident. However, instead of empowering him, he became unable to abstract and lost himself in details. Another example is the non-fiction case of 'AJ' who considered her incredible memory to be dominating her life. The trove of irrelevant information burdened her. The researchers suggested that she suffered from a yet unnamed syndrome and proposed to name it the hyperthymestic syndrome (Parker, Cahill & McGaugh 2006).

The biological memory of Funes and AJ was perceived to show similarities with the functioning of a lifelog as information was stored without regard for the distinction between the trivial and non-trivial. There is an important difference between Funes or AJ and lifeloggers. The relations between a lifelogger and his lifelog and between him and his biological memory are evidently different. A lifelogger dwelling in the past is a result of an unhealthy use of an external technology, while for Funes or AJ their ability to remember is a part of them. Funes and AJ were unable to distinguish significance. However, for lifelog technology, the lifelog is not the sole determinant of the importance of pieces of information, but the lifelogger and society have a large influence in deciding which information is

considered significant. Lifeloggers are not expected to use all of the information lifelogs provide; it seems likelier that they will select the information they consider useful or that is being promoted as useful for them by others. Being selective is common to most information technologies such as encyclopaedias, search engines, social networks, or newspapers, all of which greatly surpass an average person's ability to absorb all their information. People with different interests will value and search for other information. Hence, this variant seems to merit little weight.

Even the assumption that lifelog technology does not distinguish between the trivial and non-trivial, which was implicitly made by using AJ and Funes as metaphors, may not hold. As discussed above (*5.2.1.1 Biases*), the information that lifelogs can convey is the result of design choices and limitations to what is technologically and legally feasible. The sheer fact that information is retrievable means that someone in the process of designing the lifelog has considered the functionality to find this information sufficiently important to be included within the lifelog. The idea that lifelogs present information regardless of significance misunderstands the problem at hand; the dispute is about what information is important enough to be retrieved and can benefit the lifelogger's understanding of himself and his environment.

2) Another concern is that the additional information lifelogs offer to lifeloggers makes it more complex to understand a situation. This type of argument is not necessarily very convincing. These accounts ignore the complexity of daily life and the fact that people have little insight already into their daily goings-on. The purchase of a t-shirt, the consumption of a ready-meal, or one's daily exercise, have consequences for oneself, others, or one's environment, such as people working in sweatshops or the destruction of rainforests, but one might be unaware if one's behaviour is healthy, just, or environmentally detrimental. One may find goals, such as minimising one's carbon footprint, important, but one may not have the resources and time available to achieve these goals to satisfactory levels. This information might be available, e.g. one can find information to explain ingredients on cosmetics or food, the size of one's carbon footprint or the trading conditions in which products and services are developed. In addition, one could manually track one's behaviour, such as the brands one uses, and the size of one's carbon footprint. However, tracking one's behaviour would require resources and time an ordinary citizen might not have available. In environments where one is already inundated with information, a centralised archive that collects and organises information that is otherwise shattered and unclear could be beneficial.

149

A lifelog could perform these tasks. Figure 1 shows two screenshots of two applications that run on smartphones and that quantify activities. These screenshots might provide some idea of what a lifelog could look like. By gathering all information in a central space the lifelogger needs less time and fewer resources to access information about his life.
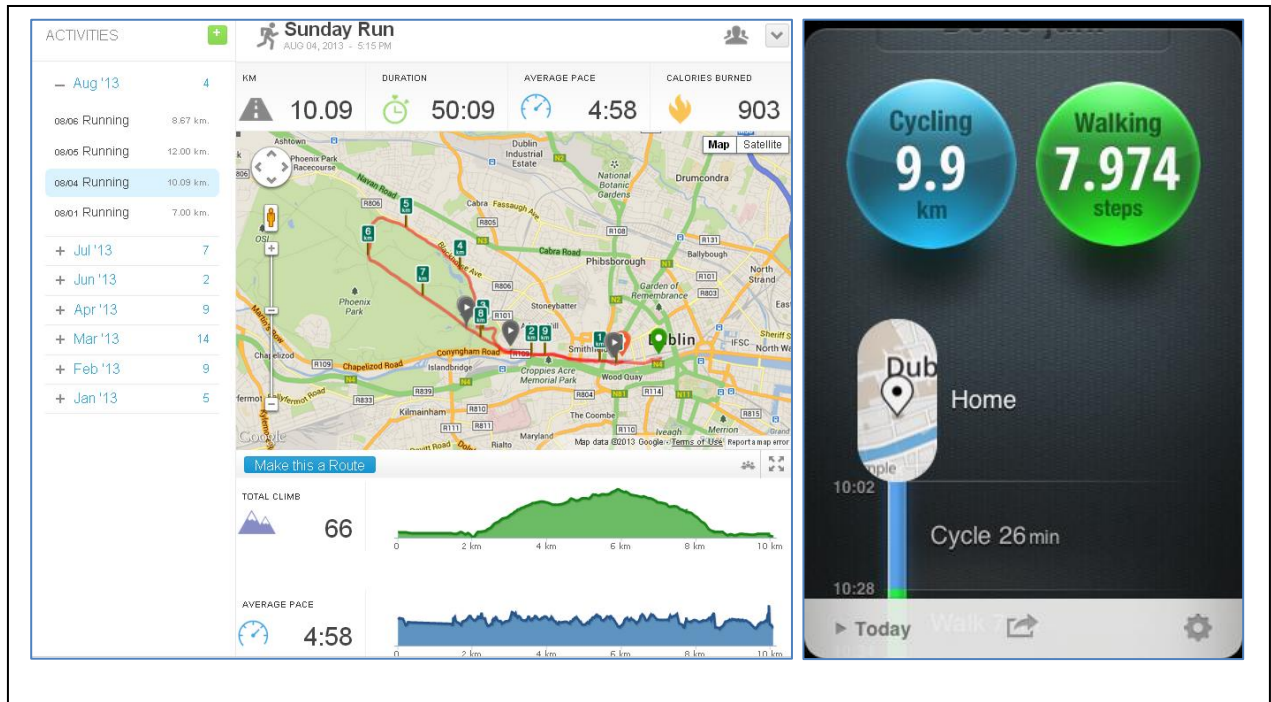
This advantage is dependent on the lifelog technology's ability to retrieve information that would otherwise be burdensome to collect.[96] Again, it requires developers to create the information that would otherwise be unavailable or time consuming to obtain. In the chapter on beneficence, examples are provided of aspects of one's life for which lifelogs might provide useful information.

2) There is a stronger variation of this concern, namely putting lifelog information into context requires time and mental skills from the lifelogger. As shown when discussing biases, lifelog information has its shortcomings that make it undesirable to be used integrally as a final and comprehensive account of the past. The availability of the digital information would require lifeloggers to consider if the information they have retrieved is, indeed, the

---

[96] There is an incentive to create information people would otherwise not obtain through lifelogs and that can be useful to them. Furthermore, lifelogs which present the lifelogger with trivial or otherwise uninteresting information are unlikely to attract popular attention. Again, if one considers Social Networking Sites or search engines, they struggle to present the user with an acceptable standard of relevant information. People refrain from using media that fail to provide them with information that satisfies their needs (Stieger et al. 2013). Social networking sites, such as Facebook and Twitter, and search engines such as Google, suffer because of the abundance of irrelevant information, such as spam – rogue advertisements -, uninteresting or irrelevant posts or search results, content farms and advertisements.

most suitable to avoid rash or unwarranted judgements and if it is the appropriate time to access this information.[97] The placing of information into the right context requires time and mental skills. Nonetheless it seems likely that lifeloggers develop some dispositions and norms about how they should use lifelog information as they would be repeatedly confronted with it and its shortcomings. Through trial and error they become more familiar with the technology so that they would not have to question the place and use of every single piece of information separately. Therefore, the complications lifelogs offer might diminish over time. However, issues with some lifeloggers unable to distinguish between the trivial and the non-trivial, showing disproportional narcissistic tendencies, will remain.

Conclusion: Lifelogs differ from AJ or Funes on two fundamental levels. First, the information lifelogs present is not the result of a biological memory that cannot distinguish between the trivial and non-trivial, but it is the result of human choices that determine which information is deemed important enough to be retrieved and technological limitations. Indeed, developers could choose to mainly provide information about important topics people may know little about: however, the probability of them doing so might be small, the creation of useful information, such as information about one's carbon footprint, might require expert knowledge for example of environmentalists and a high standard for the quality of information, both of which might demand more resources and time than a company has available. Secondly, on another level, the decision about which information should be used for reflection is the choice of lifeloggers within a community.

There is another concern: the limitations of lifelog information require the lifelogger to assess the relevance of lifelog information within a particular situation. Familiarity with the lifelog hopefully eases the decision whether to use particular lifelog information and lead to a more responsible use of lifelog technology. Nonetheless, lifeloggers may incessantly and excessively query the lifelog for information. Misuse of lifelogs is an issue that cannot be avoided with any technology and the weight of this issue is dependent on the frequency with which it occurs, something which becomes only clear when lifelogs become widely used.

5.2.1.4 Technocratic society

As discussed above, respect for autonomy requires both a respectful attitude towards the autonomy of others as well as, in some cases, positive actions to sustain or help develop other

---

[97] Moreover, the lifelogger can access this information at any time. Some moments are clearly inappropriate to access gadgets such as checking your electronic message during a romantic meal. The untimely access of digital information and the use of gadgets can have negative consequences such as harming intimacy.

people's autonomy. However, lifelogs could create an environment in which the autonomous formation of beliefs and values is discouraged.

Lifeloggers may start to rely on lifelogs for information rather than engaging with others or reflecting on information themselves. Accessing information from the lifelog in some situations will demand less resources and time and might be less tedious than engaging with the person in question or obtaining other information from other resources, especially when lifelogs offer lifeloggers prompts containing information that may be interesting for them. Moreover, lifelogs might be in many cases more reliable and precise than people are. There are similarities with technocratic governments that rely on scientific reports for policy rather than involving citizens into the process of decision-making. Lifelogs facilitate the creation of a more technocratic society in which there is less space for dialogue.

Sometimes a conflict might arise between the information a lifelogs produces and the beliefs of a person. Suppose that lifelog feeds information back to the lifelogger that the images of person 'b' doing 'X' shows that 'b' finds 'X' to be a stressful activity.[98] On the basis of this information he might prevent her from doing 'X' again even though she might convince him that she enjoys doing 'X'. He may not even contact her to inquire about her experiences because this information is now available through his lifelog. In case he confronts her she might disagree with these findings but he might try to convince her that the lifelog is often more accurate than her own perception and that she is just fooling herself. Indeed, even if no one has access to the lifelog society might promote the use of lifelogs above the use of one's mental capacities. As a result people might develop the disposition to use lifelogs rather than one's own assessments.

There are several problems with technological solutions. Brey (2006) mentions that technology might present itself in a form that makes it hard for people who lack expert understanding to criticise its output. Moreover, the data are not the result of a neutral process creating value free information but, as discussed above, the functioning of lifelogs might contain biases that result from beliefs hold by developers. As discussed above, non-material aspects cannot be measured by sensors. Judging one's past or others based on this information could lead to callous assessments (Murata 2011).

---

[98] Stress levels can be detected through heart rate monitors as stress has a number of physiological markers (Choi & Gutierrez-Osuna 2009).

Conclusion: Lifelogs could be a factor in creating an environment in which technologically generated information dominates other sources of information including people's personally held accounts. People would be faced with a situation in which their deliberative autonomy is discouraged or ignored. One solution to reduce this concern is to minimise information that can refer or be attributed to others. However, this recommendation does not completely remove the pressure from society to rely on lifelogs rather than one's own assessments. In order to address this concern, misuse has to be avoided and the limitations of lifelog technology will have to be acknowledged.

5.2.1.5   Creating a Panopticon

The reduction of privacy potentially caused by lifelogs could also affect autonomy on the level of deliberation.

Foucault has used a model for a prison designed by Jeremy Bentham, namely the Panopticon, to describe the functioning of a mechanism of power widely present in everyday life that has as a consequence that it conforms people's desires to existing norms (Foucault 1991). Essentially Foucault's description of the Panopticon can be explained in terms of privacy and autonomy. The Panopticon is a prison with a watchtower placed in the centre in which the watchmen can oversee all the cells around. These cells have glass windows leaving the prisoners exposed at every moment enabling guards to oversee abnormal behaviour while the prisoners are separated from each other's eyesight with concrete walls. The guards in the tower are not visible. At any given moment the identity of the watchmen is unknown or even if they are present at all. Inmates are separated and made observable at all times. The continuous visibility forces the inmates to internalise the desired behaviour and show this behaviour even if they are not watched, i.e. they appropriate the existing norms as if they are their own. This model enables the prison staff to exert power with a minimum of effort. This model can be applied to everyday life according to Foucault.

According to Foucault the current environment mimics the workings of a Panopticon. From birth onwards individuals are assigned properties and classification such as names, nationalities, gender, race, grades, job roles, sexuality, *et cetera* that make it possible to separate and identify individuals and keep track of their behaviour so as to improve or correct it. Foucault primarily discussed institutions that create mechanisms of power that function like the Panopticon. However fellow citizens seem to function as the watchmen in the towers as well. The proliferation of digital data and ICT allows one to capture and share information

about individuals in many public and private places while identification techniques and social platforms allow one to blame and/or reward individuals. Moreover, it is often unclear if one is being recorded and by whom and if this information is shared. After all, it is possible to record and share information without revealing who it is that shared the information. The result is that people tend to appropriate the norms that are enforced as their own.

A similar effect was described by Benson (1991) in which oppressive social structures become woven into the fabric of society to such a degree that they are unrecognisable as oppressive. He mentions the case of a female student who thinks that certain norms for appearance are connected to self-worth and therefore spends much time and money on her appearance. One might feel free and consider one's desires and beliefs as authentic, intentional and free, but in fact they are merely the product of constraints.[99] A feminist critique on autonomy holds that housewives might be content in their position because they adjust their preferences to their social environment which discourages careers rather than because of their own autonomous preferences (Christman 2009). In order to develop oneself freely according to one's own standards free from external pressures, one needs to be in an environment that can guarantee privacy to some extent (Cohen 2012).

Conclusion: Some of these problems are solved by protecting the privacy of both the lifelogger and those who they record. If lifeloggers can protect their personal information from being accessed by third parties such as companies, governments, or others, then it becomes more difficult for others to trace and judge their goings-on. In addition precluding lifelog devices and applications capturing or inferring information about others would address issues with the privacy of others. However, the information from lifelogs may still convey societal norms. Indeed, lifelogs can organise and categorise aspects of the lifeloggers'

---

[99] The reduction of privacy could even affect valuations of the worth of privacy. The standards for protecting privacy can progressively become lower society-wide. By accepting these lower standards over time, people become accustomed to lower levels eroding their desire for privacy (Schwartz 1999). It seems likely that one's desire for privacy is lowered with the gradual development of technology that creates personal information. Although empirical facts are lacking, it seems unlikely that people a few decades ago would have accepted this much personal information being available. The expectancy of privacy may have lowered gradually. In this situation people may have become 'contented slaves' regarding their privacy; people whose desires have been adjusted to an unfair situation (Day 1970). Also the lifelog company could slowly reduce the privacy safeguards it offers to the lifelogger. Additionally, this could leave users with a different issue, namely high 'lock-in costs', a term derived from economics to indicate a barrier in the market created by switching costs. For lifelogs people might either have to accept technology and waive their privacy or they would have to reject the technology and loose its functionality.

lives conform socially constructed norms, so when a lifelog is used by the lifelogger, he measures himself against these norms.

Foucault did not necessarily consider the effects of the Panopticon as undesirable. The pressure asserted on people to conform to existing norms can have positive effects when it is directed at something valuable. After all, some pressure exerted on people to internalise particular behaviour, e.g. respect the environment and do not harm the health of others, might be desirable to some degree. Indeed, this, again, highlights the need to frame lifelog information in a way that undue biases are avoided.

5.2.1.6   Summary

Five ways have been identified how lifelogs could influence the deliberative autonomy negatively of lifeloggers and others whose personal information have been captured by lifelogs. None of these issues seemed insurmountable.

The assumption that lifelogs would present unmediated reality does not seem to hold. Some biases or presupposed values are unavoidable. Biases do not necessarily make a sources of information disadvantageous to deliberative autonomy. Remember that it is unlikely that there is any source of information that is completely devoid of bias. In order for lifelog technology to advance understanding, inappropriate or ill-suited biases should be minimised or avoided and the source of information should be used appropriately by the lifelogger with observance to the limitations of the content presented to her.

Manipulation and some forms of persuasion are clearly undesirable and ought to be categorically avoided. Trying to manipulate and showing insufficient care for the interest of others means blatantly disregarding their autonomy. Manipulation is not intrinsic to lifelogs and can be avoided by securing the lifelog and by designing the lifelog with integrity.

Moreover the risk that lifelogs could actually complicate decision-making by inundating lifeloggers with information is a concern with only a limited reach. Some issues will arise, especially in the beginning, when the usefulness of lifelog information is unclear but these problems are expected to diminish when lifeloggers have become more familiar with lifelogs. Another concern is that lifelogs fail to provide information that the lifelogger would have trouble finding otherwise and that is useful to make decisions. Indeed, in case developers choose to present information that is currently complex to obtain, it can actually advance their understanding.

Another issue is that lifelogs could be instrumental in creating an environment in which people attach little value to theirs and other people's capacity for autonomous choice. Lifeloggers might rely on lifelogs rather than consult with others. This issue can be reduced by limiting the access of others to personal information and by reducing information about others within a lifelog.

Finally, reductions of privacy caused by lifelogs could increase the pressure on people to appropriate current norms within society. This issue seems largely avoided by securing lifelogs against third party access, including the company that offers lifelog services, and preventing the use of devices that capture information about others.

5.2.2 Opportunities for deliberative autonomy

The previous discussion showed the challenges lifelog information offered for deliberative autonomy; this part shows how lifelogs could advance the deliberative autonomy of the lifelogger and others.

5.2.2.1 Information about oneself

In theory the lifelog can provide the lifelogger with information that she can use to better her understanding.

Lifelogs can be used to correct misconceptions. For example, people are prone to overestimate their physical activity. This can affect health because this overestimation could lead people to exercise less than they would need to (Janevic, McLaughlin & Connell 2012; Watkinson et al. 2010). With a lifelog these misconceptions might be avoided.

The data captured can have an accuracy, which can surpass that of other people. The fact that a lifelogger becomes less directly dependent on accounts of other people might also be profitable to them, e.g. a photo of Christmas dinner may not reveal some aspects but it does show the colour of your father's shirt.[100] Therefore one avoids some accounts of information that are being influenced by self-interest, self-deception, or other distorting factors that can occur when dealing directly with others.[101] Many organisations and people may have an interest in manipulating or altering the understanding of an individual. Lifelog technology that is successfully developed with the aim to provide the lifelogger with a frank description of his past could protect the lifelogger against others. For example, a better

---

[100] Indirectly one is dependent on others to create the lifelogging technology in the first place.
[101] This is not to say that lifelogs cannot be manipulated to serve a certain purpose.

understanding of one's health could protect one against those attempting to sell products or medical procedures aiming to address a problem which may be non-existent.

The content of lifelogs might be useful to help achieve non-measurable valuable goals. Previously, it was established that lifelogs might fail to capture some information. This does not necessarily mean that lifelogs are useless when aiming to achieve goals. For example, although lifelogs might be unable to capture the quality of time spent or the meaning of time spent, the goal of spending more quality time with one's children can be achieved by using lifelogs. Part of this goal hinges on the ability to manage life more effectively so one has more time left to spend. Lifelogs could be useful in this regard as they might be able to provide information that would otherwise be difficult to obtain. For instance, a lifelog could provide one with information about travel times so one could choose the most optimal times for commuting leaving one with more time to spend with one's children. However, to profit from lifelogs, one would have to use it correctly.

By offering information to set novel goals or assess progress towards attaining goals, such as 'increase exercise', 'work less', 'use the car less', 'diminish stress levels', and 'attend a play in the theatre at least once a month', and by measuring how one is progressing in achieving those goals, lifelogs offer ways to advance or support decision-making.[102] This is especially important in contemporary Western society in which people have a multitude of options and information sources available, while information about the consequences of their choices is often scattered or for other reasons difficult to obtain. Moreover, the purchasing power people have, can lead them to buy or use goods and services which are not in theirs, others', or the environment's best interest. This can vary from leaving too much of a carbon footprint or buying food with unhealthy ingredients. For example, there is considerable information available about the nutrition necessary to sustain a healthy lifestyle, but to find this information and obtain a fair idea about one's intake can be burdensome. Lifelogs could reduce the effort needed to achieve these goals.

There may be another way in which lifelogs promote deliberative autonomy. Besides providing information that is explicitly requested by the users, the lifelog most probably also provides additional information, which users did not request or expect. This is quite similar to searching for information in a hard copy archive or in a book. The act of skimming through a

---

[102] Lifelogs could also be used to set novel goals as they provide information that one could not achieve without them.

dictionary often reveals words one had forgotten or which have connotations one was unaware of. In the digital world, even one's Google search queries can provide one with novel information one was not directly searching for. A similar thing could happen for lifelogs. When tracking one's travels, one might also obtain information about other aspects such as speed, gas burned, money spent, emission of greenhouse gasses, routes, times and weather conditions besides the routes and locations. The visibility of emissions might create awareness about the effects of one's action for the environment and allow a greater importance attached to behaviour that can affect the environment.

In addition the lifelog may customise information retrieval to the needs of the lifelogger. Lifelog technology might be made to help the lifelogger (or maybe even someone else captured by the lifelogger) obtain a greater understanding of his lifestyle. A lifelogger who has, for example set a goal to live healthier, may be proactively informed by lifelog technology that certain patterns in his current lifestyle may be harmful. These interventions of lifelogs informing one about misunderstandings could also be beneficial as they could, indeed, improve one's understanding of certain aspects of one's life.

Another way that lifelogs can support deliberative autonomy is that it can (indirectly) provide information about the way others live by them sharing their personal information obtained from their lifelogs. They can inform about alternative lifestyles and can show the result of these lifestyles. Also in this sense lifelogs may broaden one's knowledge. One will be more aware of what is out there so one can 'experiment' to see what suits one.

Finally, lifelogs may make biases more visible, which, in turn, could stimulate debate about these biases. As shown above, lifelogs may convey very partial conception that fail to account for the complexities of daily life or that promote particular existing prejudices and power relations. The solidification of these biases either in practices of censorship or feedback to the user may make them more visible and easier to combat than when those biases are only tacitly present. As a result, these biases might stir a societal discussion and the company might change its policies or the functioning of its technology, as was the case with the censoring of photos of breastfeeding and the framing of gender as a binary option. In order to experience those advantages, there must be sufficient pressure exerted on developers to change these practices or an existing want of developers to change these biases. However, sometimes these biases may be strongly supported, e.g. by conservative communities, who do not accept homosexuality and put severe pressure on the company, or by the company itself;

hence, this advantage is dependent on the willingness of developers to change a perceived bias.

Conclusion: There are limitations to the usefulness of lifelogs as a source of information, but if the information they provide is utilised wisely and they provide useful information, then they can inform lifeloggers about aspects of their lives. However, as discussed in the section about the possibility of inundating the lifelogger with information (*5.2.1.3 Overload of information*), this requires intellectual skill. Moreover, information might be biased or designed to serve the interests of others than the lifelogger (*5.2.1.2 Persuasion/Manipulation*). The usefulness of lifelogs for these purposes is not self-evident, but requires a conscious effort of developers to design lifelogs in a way that they offer constructive information to increase the lifeloggers' understanding of certain aspects relevant to live a worthy live. One could think of the values mentioned in the chapter on beneficence (*6.1.2 Value*).

5.2.2.2   Deliberative autonomy of others

There are also reasons why lifelogs can support the deliberative autonomy of others. Besides being useful as sources of personal information, one can use one's lifelog to inform others. This can support them in making autonomous decisions. This can materialise in different ways.

Sometimes, one will be unable to consult the person because that person might be temporarily incompetent. Through lifelogging, one is more likely to have other people's wishes recorded, for example through e-mails or images. The lifelogger can search the lifelog to see what decisions others made and if they expressed any wishes. The use of lifelogs for this purpose might be limited as privacy requirements demand a minimisation of information about others.

In other cases, the lifelog can be used to correct mistaken beliefs even without deploying lifelogs that capture information about others. Lifeloggers can use lifelogs to help inform others by putting forward personal information about themselves. For instance, one can use lifelogs to show how one manages one's finances, how one is able to combine work and leisure, the time one has to exercise, *et cetera*.

Conclusion: The use of lifelogs for these purposes seems limited. Privacy demands require limiting the information available about others.

5.2.3 Summary

The quote referred to in the introduction mentioned "authentic life" (Saga 2013), "your real life story, as told by the places you visited and the things you've done" (Saga 2013), and "meaningful goals" (Saga 2013). These quotes misrepresent the use of lifelogs by overstating its capabilities. The first two are blatantly untrue and misleading. Lifelogs contain very limited representations of one's past. Moreover their functioning is the result of the values and design choices by the developer in conjunction with the interests of various other stakeholders and technological limitations. In the worst case, information retrieval is being manipulated to suit the best interests of companies and investors rather than that of the lifelogger. That lifelogs do not present facts unmediated by theory and value is not necessarily a reason to consider lifelogs undesirable. Many sources of information are limited in the information they can convey.

The ability to set meaningful goals is dependent on prudential usage of the lifelog by the lifelogger. Misuse of lifelog information as the sole source of relevant information is tempting as they contain such a vast amount of information. If the lifelogger determines his decisions solely and exclusively on lifelog information, then he assumes a restrictive view on life, which is likely to impoverish his understanding rather than enrich it. Moreover, if lifeloggers begin relying on lifelog information rather than have a dialogue with the person whose information has been captured, they might create an environment unfavourable to deliberative autonomy. Finally if developers fail to secure lifelog information and allow lifeloggers to record others, a surveillance society can be created that might negatively affect deliberative autonomy.

Does this render lifelogs useless or necessarily negative to deliberative autonomy? No, in fact, a carefully designed lifelog could advance understanding and thus promote deliberative autonomy. To advance deliberative autonomy, lifelogs need to be designed with due care for security, privacy, the standard of quality for information, and the limitations of information presented to the lifelogger. Foremost, the information presented within a lifelog should provide the lifelogger with information that would be difficult to obtain otherwise and is useful when making decisions. If issues with misuse are mitigated and lifelogs are designed with integrity, lifeloggers might have an incredible source of information that can aid them to improve their understanding.

5.3 Challenges to and opportunities for executory autonomy

In this section, the focus is on the executory autonomy (or liberty). This section is divided into two parts similar to the previous one.

5.3.1 Challenges to executory autonomy

There are various reasons to believe that lifelogs might be harmful to liberty. Three actors are discussed, namely governmental agencies, corporations and private individuals that can diminish the liberty of lifeloggers by accessing and distributing personal information from lifelogs. In addition, the ramifications of bias for liberty are discussed.

5.3.1.1 Diminishments by governmental agencies

Access to personal information by governmental agencies or other public institutions, can be disadvantageous to the liberty of lifeloggers. Failures to design lifelogs as to protect privacy can have ramifications for liberty. There is an intimate relation between privacy and personal freedom.

Respect for privacy can increase liberty. According to Lessig (1999, 148) the power of a state to enforce certain laws is limited by providing weight to privacy. Lessig (1999) endorses a view in which privacy considerations and law mutually influence each other. For instance, when outlawing contraceptives, an argument is created for bedroom searches. Similarly, respecting privacy would question the coming into being of laws forbidding contraceptives as these may require violations of privacy. The landmark case of Griswold v. Connecticut (1965) illustrates this nicely. The US Supreme Court invalidated a law forbidding contraception, as the execution of such regulation would require violations of privacy.

Lifelogs facilitate surveillance because it becomes less burdensome to retrieve information. Indeed, a recent report about the activities of the Dutch secret services explicitly states that the collection of personal information is largely the result of technologies and digitised information that facilitated these collections (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten 2014). For lifelogs, the majority of searches might be based on data mining procedures and algorithms that do not burden the person being searched or the person doing the search to the same extent as body searches, house searches, or similar more physical searches would. Personal data might be harvested in bulk and subjected to algorithms without any further human involvement. The 'three hop strategy' deployed by the

US National Security Agency (NSA) in which information about connections within three degrees of separation were collected, is an example of a programme that leads to a collection of personal information, which contains information about so many individuals that it is impossible that every person has his or her personal information accessed by a data analyst.[103] Indeed, one's data can be accessed without either the authorities or the persons themselves ever knowing or noticing that the information of that specific individual has been targeted.

The checks and balances in place to protect citizens from government agencies may be insufficient, bypassed, or disregarded. Governmental agencies may want to conceal their access to particular sources of data or how they obtained certain information to become more effective in tracking people, thwarting the legal checks and balances in place to limit surveillance. In this light, a unit of the U.S. Drug Enforcement Administration unit (DEA) possibly illegitimately offered information to other enforcement agencies, which set up their own investigation concealing the DEA's involvement. The information was obtained by "intelligence intercepts, wiretaps, informants and a massive database of telephone records" (Shiffman & Cooke 2013). Another example of potentially unconstitutional government surveillance was the Florida police using a cell phone tracking device without disclosing this use to a judge to get a warrant (Wessler 2014).

Reiman (1995) considers a decrease of privacy especially troublesome for liberty in the case of minorities. Respecting their privacy would offer those minorities some personal space to decide on matters for themselves (Reiman 1995). The increased visibility of the behaviour of minorities might incite harsh social pressure (and maybe even legal measures) restricting their freedom. Privacy prevents law from coming into being that forbids behaviour that the majority group (or the ruling group for that matter) finds immoral such as homosexuality, gambling or alcohol, *et cetera*. In addition, laws and regulations might be more stringently applied to minorities diminishing their freedom. The records of minorities

---

[103] Some governments are keen to gather information about virtually anybody hoping that it becomes useful. The 'three hop strategy' entails that telephone data and Internet records can be accessed of people within three degrees of separation (Ackerman 2013). One terror suspect having 190 Facebook friends, which constitute the average amount of friends a member of Facebook has, would leave on average the data of more than 5 million people exposed (Guardian US interactive team 2013). They followed the statistics from Facebook. Of the 190 friends, 14% are friends with each other.

might be checked more often because of prejudice and other biases.[104] Often the public will be unaware of whose data are accessed. The fact that people would often be unaware of private information being accessed and misused by officials can be an issue in itself. Existing biases within society are hidden allowing prejudice to flourish. The result is that people who fit the profile are more likely to have to deal with the consequences of being investigated and as a result find their actions under more scrutiny.

Indeed, the authorities might try to gain access to the lifelog to discredit or chase specific individuals showing particular political or religious interests effectively harming political freedom and the freedom of speech. That governmental agencies do not shy away from harming reputations has recently been highlighted with revelations about the UK Government Communications Headquarters (GCHQ) using deception techniques such as smearing one's online reputation with false accusations and so-called honeytraps (coaxing people in sexual activities that compromise their position) (Greenwald 2013) or by discrediting reputations by exposing online sexual activities (Greenwald, Gallagher & Grim 2013). The latter concerned religious conservatives and none of them were accused of being involved in terror plots. These honeytraps were meant to "snare, blackmail and influence targets" (Cole et al. 2014). NBC quotes from a presentation of a secret British spy unit Joint Threat Research and Intelligence Group (JTRIG - part of the GCHQ) whose aim it was "to "destroy, deny, degrade [and] disrupt" enemies by "discrediting" activists and religious conservatists, planting misinformation and shutting down their communications" (Cole et al. 2014). The pursuit of activists could mean severely compromising political freedom and the freedom of speech.[105] Even without luring people into traps or deceiving them, access to personal information might be useful to discredit persons. The law is complex and there are many rules in place. It seems likely that a person will overstep the law in some point in time making that person vulnerable to persecution.

There are limitations to the power a government can apply set by its citizens. Too strict an enforcement of rules and regulations can provoke public anger. The accessing of information and effectively using it to enforce law are however different things. The US

---

[104] By sharing information about minorities citizens such as unfavourable statistics can show their discontent with the behaviour of minorities creating an unfavourable environment for them by demanding more repression against them.

[105] The JTRIG also went after hacktivists from a group called 'Anonymous'. This agency could target these individuals without these individuals being charged or convicted (Greenwald 2014). Their protest could even been considered a political protest that would warrant protection under the First Amendment (Leiderman 2013).

government might have data about numerous speed violations or drug abuses without ever acting on them. It is reasonable to suspect that authorities will show some reticence in acting upon the personal data as requiring too strict a compliance to the rules might lead to a dissatisfied population. Even for non-liberal countries demanding too strictly compliance to the rules in place may pose problems as privacy protects citizens against the enforcement of unpopular laws. For instance, in Saudi Arabia the Mutaween, the governmentally authorised religious police, are criticised when enforcing their interpretation of Sharia law too rigidly, such as when chasing drivers who play their radios too loudly (BBC 2012). However, governments may still be able to selectively choose its targets attempting to avoid a popular backlash and cherry pick the activists or ideologists that harm the national, the government, or an individual official's interests most.

Concerns with governmental surveillance are somewhat assuaged assuming that people might be selective in what they capture when using their lifelogs, e.g. they might choose to capture only information that can protect them against false accusations or unjust treatments, out of fear that they might incriminate themselves or others. However people may be unaware of the extent to which government agencies have access to personal information. Governments may be able to crosslink and triangulate data in ways activists, dissidents or other people may not have foreseen. In addition, others, who are unaware or indifferent to the risk they pose, may capture information that can be used to incriminate those around them.

Conclusion: Lifelog technology could facilitate surveillance. The facilitation of distribution and access of personal information make it less burdensome for government agencies to persecute, harass, or search people. Moreover, the surveillance can happen covertly without anyone being aware of privacy breaches. The latter is particular worrisome when there are insufficient checks and balances in place to control the behaviour of the authorities. Issues with surveillance are largely due to failure to secure lifelog data from being accessed by government agencies. Compliance with recommendations for privacy, such as keeping lifelog data in the possession of lifeloggers rather than lifelog companies, would largely prevent these issues from occurring. Lifelog data in the possession of lifeloggers would have to be subpoenaed individually by government agencies, which requires more time and effort than large data swoops.

5.3.1.2 Diminishments by corporations

Corporations can also affect one's personal freedom. People are dependent on corporations in several ways. Corporations can offer services and products vital for people to live a worthwhile life. Also people can be dependent on corporations for income and employment.

Corporations can limit or increase personal freedom by providing financial or other incentives to steer behaviour.[106] This shows with the profiles they establish which determine one's eligibility for certain products (Gandy 2006). Data brokers can determine one's eligibility for loans as well as offer information for background checks. This can have far-reaching effects on one's opportunities and can affect one's chances on the job market. In the case of insurers, most people depend on them for affordable health care. Access to healthcare can be essential to maintain one's bodily health, which, in turn, is necessary to autonomously shape one's life (Nussbaum 2003). Insurance companies could increasingly deter individuals from unhealthy behaviour with material penalties, by increasing premium costs or decreasing coverage. The U.S. Patient Protection and Affordable Care Act (PPACA) allows employers to charge employees with variable health insurance rates depending on their diet, exercise and other wellness-related choices. Indeed different kinds of companies can choose to exclude people or adjust their products on the basis of personal information.

Just as corporations can model their product and its price to personal information companies might also use personal information for their workforce. It is increasingly common practice to judge the suitability of future employees by their online profiles or digital data. Approximately 45% of HR decision makers used social media in the recruitment process including screening the candidates (Broughton 2013). Credit card payments are now being used by employers to assess future employees, something which was probably was not foreseen by those taking loans a decade ago (Carney 2013).

Corporations could also use personal data to punish existing employees. Ashley Payne can be used as an example. She lost her job in a public high school in Georgia, USA, when photos that pictured her drinking a complimentary Guinness and a glass of wine at the Guinness Storehouse and an announcement to attend an event with a profanity in the name came into the hands of the school management (CBSNews 2011). Both the photos and the announcement were only visible to her friends on Facebook, i.e. Payne had consented that

---

[106] They might have an immense archive of personal information that can be used to discredit one. Also there financial power might give them an advantage towards the average consumer.

those people could access this information. She wanted the photos only to be viewed by 'friends', people within her social network. No strangers had access to this information, but one or more of the people that had to be trusted to keep this information confidential decided to show this information to her management and undermine her reputation. The posts proved sufficient for the school's management to ask for her resignation. This shows both the difficulty to control the spread of information as well as the consequences of the spread of information. One has to bear in mind that one's behaviour and its digital traces could severely affect one's possibilities.

There are potentially huge issues with transparency when corporations use data. The way corporations use and process personal information might be opaque. Maybe corporations begin using complex algorithms to process these large datasets. These algorithms may obscure decision-making and make it more difficult for lay-people to dispute their decisions. Even employees within the organisation may not know how the algorithms function or what factors are considered relevant (and their relative weight). For instance, Google's algorithms are so complex that it is impossible to tell how the variables affect personalised search results (Pariser 2011). In case those algorithms become more pervasive, people become increasingly dependent on a system they do not understand and which can determine their eligibility for services and products (Morozov 2013). The inability to understand the system also impedes on their ability to criticise it (Brey 2006). Some of the recommendations they provide might be based on distinctions that one would ordinarily find discriminatory such as those which are partly based on the fact that one lives in a neighbourhood in which predominantly African Americans live (Gandy 2006).

Conclusion: The integration of lifelog data within the daily operations of a corporation can become common practice if lifelog information is readily available. The data can be used to reward or penalise behaviour. Although sometimes it may be permissible for companies to stimulate behaviour, e.g. some incentives to improve productivity or health may be warranted, corporations could penalise behaviour too harshly or fail to consider the interest of the consumer or employees and only maximise their own. Challenges with corporations having access to lifelog information are partly solved by protecting the privacy of people. There should be technological solutions in place to prevent companies from accessing and distributing lifelog data.

5.3.1.3 Diminishments by other private individuals

Also private individuals can infringe on personal freedom. Whereas government agencies are often forced to show some restraint towards the sharing of personal information about private individuals in order to enforce moral standards – especially in liberal countries -, private individuals can share information about themselves or others with value judgements on platforms such as YouTube, Facebook, Twitter, TheDirty.com or Instagram without having to exercise the same reticence. Private individuals are more likely to share information about others they consider distasteful, immoral or otherwise notable even when that behaviour falls within the legal limitations of the law.[107] Indeed, the threshold for sharing information is so low that everyday life occurrences with little to no newsworthiness have a platform. Consequently, one can find photos, videos, gossip, and audio recordings annotated with captions and commented on by others about people who are behaving only slightly different from the norm.

These pieces of information have real life consequences. In China (and arguably other parts of the world) the phenomenon of human-flesh (or human powered) search engine exists (Downey 2010). A human-flesh search engine is an ad-hoc group effort between (potentially) thousands of people who try to identify a person in real-life based on clues found on the Internet. These searches can be provoked by moral outrage. This was the case when a video got noticed by a wider audience of a woman killing a kitten using her heels. She aroused the anger of a mob of 'netizens' – users of the WWW - who tried to identify her and the cameraman in real life in order to punish them. The mob of vigilantes succeeded and they uncovered details of their lives such as their real names, phone numbers, employers and home town within six days. As a consequence, both lost their jobs and she had to move to another city. Despite the immorality of their behaviour, their acts were in fact legal. This example may trigger the idea that only acts that are morally highly questionable are punished, but also more innocuous behaviour can have consequences outside the digital realm as the example of Ashley Payne previously showed (*5.3.1.2 Diminishments by corporations*).

Especially the ubiquitous threat of being recorded requires one to behave differently because one would need to assess one's behaviour in the eyes of other people monitoring one

---

[107] According to Gavison "privacy … prevents interference, pressures to conform, ridicule, punishment, unfavorable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform them (Gavison 1980, 448)."

(Reiman 1995, 38). Aronson (2008) used the term 'conformity' to describe an effect similar to this. It seems unfair to request every person to remain unfazed by the gaze of others and the restraints they impose by their gaze and carry on as if they were alone or if others cannot harm them.[108] Suppose one expresses doubts about one's religious beliefs during a temporary lapse of faith while living in a strongly religious community. If a recording about these expressed doubts reaches others, one could be forced into the awkward position of having to explain one's thoughts even when they might reflect poorly on one's current values and beliefs. Others might require explanations from one that one is not ready to provide. Moreover, there might be an increased need for consistency with previously held beliefs or behaviour. A change of position would require an explanation to others noticing this change of mind risking that one is being considered inconsistent. As a result, one might be inclined to conform to existing practices regardless if one desired to do so. This has far-reaching consequences for people's personal development. One ends up with less freedom to develop oneself in new and original ways that diverge from existing everyday life.

Issues regarding executory autonomy may not only stem from recording the imagery of others or the targeting of specific individuals or communities. Another way in which lifelogs can limit liberty is that their kind of information could become increasingly prominent when reflecting on matters. It seem likely that lifeloggers will not only use particular lifelog information to judge themselves, but that the insights they gain from lifelogs will also be used to judge others. For example, a lifelogger becoming increasingly aware that eating 'X' is unhealthy, will most likely inform others, such as her friend or her partner, that they should not eat 'X'. Sometimes these judgements are desirable, as they might force us to live healthier; however, due to the limitations of lifelog information, these judgements may fail to acknowledge differences in values and beliefs held between people and the ways in which one may sacrifice health or other tangible aspects of one's well-fare in order to achieve particular goals one considers worthwhile, which may not be shared by others in one's environment.

Due to the abundance of digital information, a stronger emphasis might be put on conditions that can be measured, e.g. health, financial costs, the environment, etc, than on non-measurable aspects. Social, religious, aesthetic, cultural and moral dimensions cannot be captured by sensors. In case lifelogs are used for normative evaluations of behaviour, lifelogs

---

[108] This might be another argument to limit the use of lifelogs to competent adults who are in general more capable of withstanding social pressure.

could skew judgements. Costs and inefficiencies can become increasingly visible through lifelogs and, as a consequence, will have to be increasingly accounted for when tensions arise between these costs and the non-measurable worth of these things. The costs of holy days or not working for religious reasons on Sunday may be more difficult to explain to oneself or others when information about their importance cannot be captured while information about their costs is prevalent.

An additional complication may be that some of these aspects promoted by lifelogs may be considered good to anyone and society as a whole, such as health or the protection of bodily integrity. In the chapter on beneficence, a list of benefits of intrinsic worth is provided. Improvements for health and bodily integrity are often welcomed. However, health and bodily integrity are not the only things of value. A too narrow focus on either health or bodily integrity may impoverish one's life. Often minor trade-offs to health are made, e.g. spend a night working instead of sleeping, or risk to bodily integrity are taken, for things that are valued more but which value might be more difficult to measure, such as intellectual satisfaction or the maintenance and establishment of friendship. In case these trade-offs are made more visible and potentially penalised, e.g. with social disapproval or allegations of negligence, one's ability to shape one's life is impaired. In fact, the use of recording technology can impair the realisation of particular values and activities. In Western society, it is fairly acceptable to take photos in most places including holy ones; the relevance and acceptability of these actions might not be evident within other cultures or to some people. Nonetheless, the presence of recording technology may be detrimental to certain values or activities. An example of this is the establishment of friendships, which can be a practice that requires intimacy and, for that reason, an absence of recording technology. The refusal to let others take photos has to be explained in a society which attaches no destructive symbolic value to recording technology.[109] However, it may be difficult and burdensome to explain the importance of these non-measurable aspects, while the measurable advantages are less difficult to show.

Conclusion: By using lifelogs and similar technologies imprudently, a society may be created that fails to allow for practices serving non-measurable values or that provides too strong an emphasis on measurable aspects. Again, most of the issues seem to arise from a possible failure to address concerns relating to privacy. If developers fail to address privacy

---

[109] Indeed, even the freedom not to use a lifelog might be compromised. This issue is discussed below (7 *Autonomy*).

concerns, these issues are more likely to occur. In addition, lifeloggers can exert some control over the functioning of lifelogs. The use of lifelog technology will be mediated by social norms and regulations, which may alleviate concerns with biases. Different cultures will find different uses for and meanings to lifelogs. An example is the use of smartphones, which might become pivotal lifelog devices. These phones are used by people from different cultural backgrounds, but the way in which they are used, adopted, and designed is said to vary within different cultures (IAB & IIAC 2013). Nonetheless, despite measures to protect privacy and control over the use, the prominence of measurable information may draw away attention and resources to other relevant aspects.

5.3.2 *Opportunities for executory autonomy*

There are also reasons why lifelogs might be favourable to liberty. Three of them will be discussed.

5.3.2.1 **Protection against authorities**

There are several ways in which lifelogs could protect citizens against authorities. Three examples are provided of how lifelogs could improve the liberty of citizens towards their authorities.

1) As discussed above, many sources mention sousveillance as an advantage of lifelogs for autonomy (*3.2.2.1 Citizen empowerment*). The use of lifelogs might facilitate sousveillance as proposed by Steve Mann (Mann 2002; Mann 2004). Sousveillance is thought to alleviate issues with surveillance. Sousveillance is the monitoring of authorities by individuals. The concept of authority is interpreted broadly. Even companies are considered authorities. The Rodney King Tapes 1991 and the following LA Riots in 1992 are an early example of sousveillance. The Arab Spring of 2010 in which people in multiple countries in the Arab world protested against their regime is a more contemporary example.[110] Although these examples are about monitoring governmental authorities such as the army and the police force, sousveillance is also the monitoring of managers by employees or the monitoring of staff by customers.[111] Consumers can profit from sousveillance as

---

[110] Sometimes corporations, governments, or communities react to injustices by taking measures to prevent them because they consider these to contradict their values and purposes or because of popular outcry. Sousveillance might be most forceful when authorities are relatively just as evidence of abuse of power or injustice might require them to tackle the issue rather than to ignore or suppress the people sharing this information out of fear of losing their moral standing.

[111] Mann even extends it to customers filling out questionnaires about the staff for managerial purposes, which is somewhat puzzling because this seems a form of indirect surveillance. By providing questionnaires the

misbehaviour by companies can be shared and targeted. Steve Mann has reported abuse by McDonalds staff recorded with a wearable camera (Mann 2012).

David Brin (1998) also seems to endorse something similar to sousveillance. He describes a scene in which a shoplifter is "taking into custody gingerly with minute attention to ritual and rights, because the arresting officer knows that the entire process is being scrutinised by untold numbers who watch intently, lest her neutral professionalism lapse" (Brin 1998, 4). Sousveillance, according to Mann, is the recording of authorities by subordinates who could privately hold these recording and share them when necessary. Instead of using an *ad hoc* collection of personally held devices, which seemed the case with Mann, Brin suggests a scenario in which surveillance is collectively organised with security cameras that are available to anyone.

2) There are also other ways in which lifelogs can provide protection (O'Hara, Tuffield & Shadbolt (2009). Lifelogs can offer the lifelogger information that they can advance to refute allegations of governments or show malicious behaviour by them. They serve as some sort of 'alibi'. Sometimes lifelogs might be used to prevent further confrontations with governments. The latter was the case for Ai WeiWei and Hasan Elahi who felt threatened or burdened by the government and chose to share their personal information on a website partly to avoid further harassments (Branigan 2012; Ted 2011).[112] Protection against governmental interference can even be achieved without capturing information about others. Hasan Elahi provides pictures without other people on them (Ted 2011).

The reach and use of this kind of protection for other people can be questioned. Elahi and WeiWei were directly and repeatedly targeted by government agencies. Not many people will face the same harassment as they did. Moreover both seemed to attract attention of the public or were already known, so it seems more likely that people would actively monitor and

---

customers gains some power over the staff as they can judge the staff. However these questionnaires are used by the management to judge the employees.

[112] Hasan Elahi shares his GPS coordinates, debit card transactions, and photos (without other people on them) on this website http://trackingtransience.net/. The sharing of his information was a reaction on being repeatedly questioned by the FBI as a terrorist suspect. Elahi became afraid that he could not provide all the information they demanded of him and decided to proactively make this information available. WeiWei introduced WeiWeiCam, a lifecasting project that used webcams to stream his life in real-time on the Internet, to inform his environment about his safety after having been arrested a year ago by the Chinese authorities (Branigan 2012).

pursue their well-being than that of an ordinary citizen.[113] However, it seems unclear if every other ordinary person would get the same attention. What if it becomes know that some person in China has disappeared under vague circumstances? The media attention and public pressure on the authorities would not be as severe as when WeiWei would under suspicious circumstances disappear. Nonetheless, lifelog data may, under some conditions, be useful to show the lifeloggers innocence in times of suspicion.

3) Information can be used to inform others and address existing injustices. This function is similar to sousveillance in the sense that by capturing your life you also capture the living conditions you are in. It is dissimilar because you do not necessarily have to record the behaviour of others. Private individuals can use their lifelogs to compare their situation with their peers or share their information with others who can help them.[114] In other cases, the lifelogger may share information he considers harmful. For example, an employee may use information from his lifelog to show his poor working conditions in the hope that the sharing may aid to changing these conditions. Lifelogs can capture information with little to no resources or time required from the lifelogger allowing more people to capture this information than when research projects need to be set up.

Conclusion: Although one may be empowered in some ways by lifelogs, they will not outweigh all liberty concerns associated with surveillance. As discussed above (*3.3.1.2 Questioning sousveillance*), surveillance is often exercised at places inaccessible to lifelogs. If authorities access lifelogs, lifeloggers are expected to have insufficient insight into how information is digitally processed. Furthermore, as Morozov (2011) argues, authorities can squash protests by monitoring early signs of unrest captured by accessing digital data. In fact, according to him, digital technology could have a negative effect on emancipatory forces as was discussed before (*3.3.1.2 Questioning sousveillance*). Government agencies may enforce structural access to sources for digital data to target activists or terror suspects. There is indication that US and UK government agencies are pressing developers to purposely design weaknesses within encryption to secure data to make data more easily accessible to them (Ball, Borger, Greenwald 2013: Sanchez 2013). Moreover, their funding, technological know-how and authorisation provide them with incredible opportunities to encrypt and access

---

[113] Both Elahi and WeiWei were one of the first to publicly share digital images of their lives on the Internet to protect themselves against the authorities and already had a public profile, which might also be a reason why they gathered more attention.

[114] Admittedly this can also reinforce existing injustices. Some acts or ideas can become accepted as unavoidable, when evidence that it is deeply embedded into society emerges.

personal data that are unmatched by ordinary citizens. In 2013 the NSA received almost $11 billion and the US government invested $52 billion in total that year in surveillance (Gellman & Miller 2013). In addition, Morozov (2011) argues that the visibility of illegitimate governmental actions is insufficient to mobilise people. Furthermore sousveillance may do little especially if abuses are being condoned by a large part of the population. This is arguably the case in Russia with LGBT rights and violence against that community (Human Rights Watch 2013). As public opinion is very much against their rights, public videos have little effect. In contrast, videos of abuse are made public in order to deter members of the LGBT community to express their sexuality. Hence, although sousveillance and other forms of information sharing can be powerful, they seem insufficient to create more freedom overall.

If governments could be excluded categorically from accessing personal information, then the effect of lifelogs would likely improve the lifelogger's freedom vis-à-vis government agencies; if lifelogs do safeguard privacy - do not capture information about others and secure data against third party access, then having an archive with personal information can be used to better the situation in which one finds oneself in relation to authorities. Indeed, this underlines the importance of protecting privacy. However, in the current environment in which governments show little discretion in accessing and sharing personal information and in which perfect security seems still a distant ideal, it is highly questionable if developers can sufficiently protect privacy.

5.3.2.2   Protection against other private individuals

Similar to protection against the authorities, lifelogs can also provide information that can protect lifeloggers against other private individuals. People may be deterred from infringing other people's freedom knowing that they might be recorded. In addition, the information recorded can be shared to address undesirable behaviour or practices.

Lifelogs could have a function similar to security cameras. People sometimes protect their houses with security cameras to capture evidence that can be used to trace intruders or deter potential intruders from entering the house. For the same reasons lifeloggers could wear cameras to protect themselves against abuse from others. Already in some regions people are protecting themselves by equipping their cars with dashcams (dashboard cameras), which are cameras that capture what happens in front of the car. These dashcams can be useful in case of accidents as the driver has evidence to show to the authorities and insurance companies.

Dashcams are also used to protect drivers against false claims. False claims are perceived as a significant worry in some parts of the world (Barry 2013; George 2013). In daily life, by using lifelogs one could capture information about others that are compromising one's freedom such as people who discriminate, bully, or otherwise hinder one. By being provided access to lifelog content of people in need, such as minorities that are discriminated against, one will obtain incredible information about the difficulties and support they encounter. Indeed even when one does not capture the imagery of others information about body signs, GPS, *et cetera* can reveal a great deal about the lifeloggers interactions with their environment. This information could be taken to the relevant authorities, other organisations, or to other private individuals through online social platforms, who could react to it.

Conclusion: This is not to say that lifelogs that capture personal information about others predominantly increase the liberty of private individuals. In general recording others is more likely to infringe rather than augment the liberty of individuals. As discussed above (*5.3.1.3 Diminishments by other private individuals*), the capturing and sharing of personal information about others and the associated reduction of privacy can have tremendous negative effects on personal freedom. Moreover, these recording may lead to vigilantism (e.g. human flesh search engines), witch hunts, or conformism. In addition, people may edit content or the data shared outside the context provides a distorted account of the affairs. The advantage does not come close to balancing out these concerns. Furthermore, people often experience safety without having to wear recording devices. The need for lifelog devices is often not urgent.

5.3.2.3   More tolerant societies

Almost paradoxically, the consequences of norms being imposed on people are not necessarily negative for personal freedom. The prevailing social and legal norms may demand tolerance and allow personal freedom instead of intolerance and restrictions. This can for example materialise in some people or communities being condemned for being racist or homophobic and pressure exerted on individuals to allow people some liberty. Thus, existing social norms could demand the creation of an environment in which heterogeneous lifestyles can flourish. Although one might enjoy less freedom on the level of deliberation – certain values and beliefs are discouraged and punished, e.g. racist ideas – on the level of execution people might on balance enjoy more freedom due to these structures – e.g. certain groups may not be marginalised because racist ideas are suppressed. Moreover the fact that information about behaviour becomes more widespread could make it more difficult to

prosecute. It may become too burdensome to blame everyone for petty wrongdoings. Examples of this in law are tolerating small amounts of illegal substances.

Conclusion: The main issue is that social norms can just as easily be harmful, for example when the norm is homophobia. In Nigeria, Uganda and Russia the rights extended to the LGBT community seems to have been lowered while those countries have experienced an increase in IT. There seems no reason to *a-priori* assume that the prevailing rules are *necessarily* good or desirable and, in fact, they can be wrong and undesirable. In addition, officials may selectively prosecute those individuals who they desire to disrepute. Nonetheless in tolerant societies the enforcement of some social norms may actually be beneficial to the majority of people.

5.3.3 Summary

It seems yet unclear if lifelogs would actually enhance or decrease personal freedom. Much will depend on the context in which they are used and if they are made to conform to safeguard privacy. There is a checklist provided as an appendix that allows for a swift identification of potential concerns regarding autonomy (*Appendix B: Checklist for autonomy*).

An important factor is the ability of lifelogs to comply with demands made to protect the privacy of the lifelogger and that of others. Already when discussing deliberative autonomy it became evident that privacy was required to prevent pressure exerted on people to conform. For liberty privacy might be even more important in many situations. The negative effects on liberty are almost invariably caused by failures to protect privacy with the exception of some of those that are caused by the biases inherent to lifelog information. If government agencies, corporations, and others could be categorically excluded from possessing information *and* if the capturing of information about others is limited, then the potential for reductions of liberty would be greatly diminished. Though, some issues stemming from shortcomings in lifelog information unrelated to privacy will persist, such as people judging themselves and other based on content that fails to convey relevant information.

Indeed in the event lifelogs are designed with due care for privacy they could also have an emancipatory effect. Revelations about abuses by companies, other private individuals or government officials might change these unfair existing practices. Even

lifelogs in which information about other people than the lifelogger is minimised or avoided can be used to show unfavourable working/living/political conditions. Moreover, for some people recording themselves might actually be a way to protect them against government agencies or others that persecute them. This group is currently believed to be quite small.

5.4 Recommendations

The recommendations to alleviate concerns regarding privacy had control as their focal point; recommendations to advance autonomy evolve around a reasonable standard of quality for information and mitigating concerns regarding privacy. The main concerns for deliberative autonomy are biases, invested interests, or manipulation and misuse by the lifelogger. Concerns regarding liberty are mostly dependent on the ability to maintain privacy. Recommendations to safeguard privacy were presented in the previous chapter. Again, compliance with these recommendations may hurt commercial interest in the short term but might be a more viable strategy for the long term as it promotes trust. Below ten recommendations are provided to tackle the issues with autonomy.

1. Quality of information: The standard of quality for information should be high, which means that the presented information should be accurate *and* the content presented by lifelogs should present information that is helpful for the lifelogger to understand more about her past. The latter can be achieved by providing information about import aspects of one's life, such as health or one's carbon footprint, rather than solely presenting trivialities. Developers could use the list of values provided below in the chapter on beneficence to identify aspects of interest (*6.1.2 Value*).

2. Prevent manipulation: Manipulation should be categorically avoided. The lifelog company should not deceive or mislead the lifelogger. The company should also protect the lifelogger against other trying to alter the functioning of lifelogs or their content in order to manipulate lifeloggers.

3. Explain claims: The lifelogger should be informed about the theories underlying information presented to the lifelogger. In addition the data sources used to obtain this information need to be explained. It may be unclear to the lifelogger why certain information is presented and what theories and data sources have been used. For example, in case lifelogs provide feedback about health, the lifelogger should be able to retrieve information about the justification for claims.

4. Indicate when information is being influenced for commercial interest: When querying a lifelog or being presented with lifelog information, it should be clear when the results are being influenced by commercial interests and if there are other parties that have vested interests in the lifelog content, such as advertisement companies.

5. State what information is excluded: In a lifelog some information is most likely filtered out or deemed inappropriate. The developers should indicate clearly what they deem as unsuitable to be held within the lifelog. The so-called rules of the house should be clear.

6. Security: Lifelog information should be protected against second and third parties that manipulate information or aim to obtain information so that they can exert their influence on the lifelogger. As already became clear in the chapter on privacy, security is pivotal when designing a lifelog.

7. Sensitivity to bias: The lifelog should be designed in a way sensitive to bias and in a way that identified undesirable biases can be addressed. Bias cannot be completely avoided. However, it is possible to identify and address some biases, e.g. the extension of gender options within Facebook to accommodate users that feel unacknowledged. Ideally, developers have created channels through which they can identify and address potential biases to avoid those that are undesirable.

8. Avoid presenting information as undisputable facts: The lifelogger should be warned that the information presented by lifelogs is the result of estimates and that the lifelog is fallible. The intrinsic shortcomings of the information should be accounted for. The presentation of lifelog information should reflect these limitations.

9. Avoid normative content: Developers of lifelogs should avoid intentionally using terminology or a lay-out that either promotes or discourages particular behaviour without notifying the lifelogger *and* the content should not harm the interests of the lifelogger.

10. Address concerns regarding privacy: Respect for privacy and respect for autonomy seem intertwined as a failure to respect either one of them most likely results in a failure to respect the other. Recommendations to alleviate privacy concerns are provided in the previous chapter. These recommendations should be complied with.

5.5   Conclusion

In contrast to issues related to privacy, the effect of lifelogs on autonomy does not univocally make the principle respect for autonomy a *prima facie* consideration in favour of or against lifelogs. There are reasons to argue that lifelogs could harm the autonomy of lifeloggers and non-lifeloggers. These violations of autonomy are sometimes avoidable, such as failing to explain commercial interests or failing to stress that lifelogs are fallible, while others are intrinsic, such as biases and the technocratic conception. These concerns are serious enough to warrant consideration. Moreover, a failure to respect privacy seems to lead to many concerns regarding liberty. If concerns with privacy can be avoided, lifelogs seem a tool to improve the liberty of lifeloggers.

During the discussion on the potential negative effects of lifelogs on deliberative autonomy, it became quite clear that some issues are inherent to many sources of information, while others were avoidable or could be minimised either through usage and/or development. Although lifelogs are a limited source of information, their information could actually advance the deliberative autonomy of its users. However, its effect will largely depend on the design and usage of lifelogs.

In addition, it has become clear that there are positive and negative consequences for executory autonomy. Most of the concerns are caused by a failure to protect privacy. In case lifelogs are developed with due care for privacy, most issues with executory autonomy seem mitigated. Furthermore some advantages to executory autonomy are not dependent on technology that captures information about others.

Finally, there have been ten recommendations provided to address issues with autonomy and reap the benefits for autonomy.

Bibliography

Ackerman, S. 2013. NSA warned to rein in surveillance as agency reveals even greater scope [Online]. *The Guardian.* Available from: http://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing [Accessed 02-11-2013].

Aronson, E. 2008. *The Social Animal.* New York: Worth Publishers.

Ball, A.L. 2014. Who Are You on Facebook Now? [Online]. *The New York Times*. Available from: http://www.nytimes.com/2014/04/06/fashion/facebook-customizes-gender-with-50-different-choices.html [Accessed 24-04-2014].

Ball, J., Borger, J. & Greenwald, G. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 09-09-2013].

Barry, C. 2013. Why Do Russians Film Their Car Accidents? Available from: http://www.slate.com/articles/technology/technology/2013/02/chelyabinsk_meteor_videos_why_do_russians_film_their_car_accidents.html [Accessed 12-09-2013].

BBC. 2012. *Saudi Arabia religious police chief announces new curbs.* Available from: http://www.bbc.co.uk/news/world-middle-east-19819791 [Accessed 29-05-2013].

Beauchamp, T.L. & Childress, J.F. 2009. *Principles of Biomedical Ethics: Sixth Edition*. New York & Oxford: Oxford University Press.

Benson, P. 1991. Autonomy and Oppressive Socialization. *Social Theory and Practice*, 17(3), pp. 385–408.

Benson, P. 1994. Free Agency and Self-Worth. *The Journal of Philosophy*, 91(12), pp. 650-668.

Berlin, I. 1958. Two Concepts of Liberty. IN: Berlin, I. 1969. *Four Essays on Liberty*. Oxford: Oxford University Press.

Bijker, W., Pinch, T. & Hughes, T. 1987. The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. Cambridge: Massachusetts Institute of Technology Press.

Borges, J.L. 1962. *Ficciones*, translated by Anthony Kerrigan, New York: Grove Press.

Branigan, T. 2012. Ai Weiwei installs studio webcams for supporters and security services [Online]. *The Guardian.* Available from: http://www.guardian.co.uk/artanddesign/2012/apr/03/ai-weiwei-webcams-supporters-security-services?newsfeed=true [Accessed 19-05-2013].

Brey, P. 2006. Ethical aspects of behavior-steering technology. *IN:* Verbeek, P.P. & Slob, A. (eds.) *User Behavior and Technology Development*, Dordrecht: Springer, pp. 357-364.

Brin, D. 1998. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Cambridge: Perseus Books Group.

Broughton, A., Foley, B., Ledermaier, S. & Cox, A. 2013. *The use of social media in the recruitment process*. Institute for Employment Studies: Brighton.

Carney, M. 2013. You are your data: The scary future of the quantified self movement [Online]. *Pando Daily.* Available from: http://pandodaily.com/2013/05/20/you-are-your-data-the-scary-future-of-the-quantified-self-movement/ [Accessed 01-08-2013].

CBSNews. 2011. Did the Internet Kill Privacy? Available from: http://www.cbsnews.com/8301-3445_162-7323148.html [Accessed 20-05-2013].

Choi, J. & Gutierrez-Osuna, R. 2009. Using Heart Rate Monitors to Detect Mental Stress. *IN: Proceedings of the 2009 Sixth International Workshop on Wearable and Implantable Body Sensor Networks*, June 03-05, 2009, pp. 219-223.

Christman, J. 1991. Liberalism and Individual Positive Freedom. *Ethics*, 101(2), pp. 343-359.

Christman, J. 2009. Deontological Ethics [Online]. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Spring 2011 Ed. Available from: http://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=autonomy-moral/ [Accessed 20-03-2013].

Clowes, R.W. 2012. Hybrid Memory, Cognitive Technology and Self. *The proceedings of the AISB and IACAP World Congress 2012.*

Cohen, J.E. 2012. *Chapter 5: Configuring the Networked Self*. Available from: http://www.juliecohen.com/page5.php [Accessed 19-05-2013].

Cole, M., Esposito, R., Schone, M. & Greenwald, G. 2014. Snowden Docs: British Spies Used Sex and 'Dirty Tricks' [Online]. *NBCNews.* Available from:

http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091 [Accessed 26-02-2014].

Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten. 2014. *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD* [Online]. Available from: file:///C:/Users/jacquet2/Downloads/38Toezichtsrapport%20gegevensverwerking%20telecommunicatie.pdf [Accessed 12-03-2014].

Day, J. P. 1970. On Liberty and the Real Will. *Philosophy*, 45(173), pp. 177–192.

Dib, L. 2008. Memory as Concept in the Design of Digital Recording Devices. Altérités, 5(1), pp. 38-53.

Dib, L. 2012. The Forgetting Dis-ease: Making Time Matter. *A Journal of Feminist Cultural Studies*, 23(3), pp. 43-73.

Downey, T. 2010. China's Cyberposse [Online]. *The New York Times.* Available from: http://www.nytimes.com/2010/03/07/magazine/07Human-t.html?pagewanted=all&_r=0 [Accessed 25-05-2013].

Dworkin, G. 1972. Paternalism. *The Monist*, 56(1), pp. 64-84.

Dworkin, G. 1976. Autonomy and Behavior Control. *The Hastings Center Report*, 6(1), pp. 23-28.

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

Facebook. 2013a. *Does Facebook allow photos of mothers breastfeeding?* [Online]. Available from: https://www.facebook.com/help/340974655932193/ [Accessed 23-08-2013].

Facebook. 2013b. *Facebook Community Standards* [Online]. Available from: https://www.facebook.com/communitystandards [Accessed 23-08-2013].

Foster, C. 2009. *Choosing Life, Choosing Death: The Tyranny of Autonomy in Medical Ethics and Law*. Portland: Hart Publishing.

Foucault, M. 1991. *Discipline and Punish: The Birth of a Prison*. London: Penguin.

Frankena, W.K. 1973. *Ethics.* Englewood Cliffs: Prentice-Hall, Inc.

Frankfurt, H.G. 1971. Freedom of the Will and the Concept of a Person. *The Journal of Philosophy*, 68(1), pp. 5-20.

Friedman, M. 2003. *Autonomy, Gender, Politics.* New York: Oxford University Press.

Fuchs, A.E. 2001. Autonomy, Slavery, and Mill's Critique of Paternalism. *Ethical Theory and Moral Practice*, 4(3), pp.231-251.

Gandy, O.H. 2006. Data-mining, surveillance and discrimination in the post-9/11 environment. IN: Haggerty, K. & Ericson, R. (Eds.), *The new politics of surveillance and visibility*, pp. 363-384. Toronto: University of Toronto Press.

Gavison, R. 1980. Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), pp. 421-471.

Gellman, B. & Miller, G. 2013. U.S. spy network's successes, failures and objectives detailed in 'black budget' summary [Online]. *The Washington Post*. Available from: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html [Accessed 09-09-2013].

George, A. 2013. The Best Dash Cam. *The Wirecutter*. Available from: http://thewirecutter.com/reviews/best-dash-cam/ [Accessed 12-09-2013].

Gerster Trocola, M. 2005. Breastfeeding in Public. *NEW BEGINNINGS*, 22(6), pp. 238-243.

Giles, J. 2011. US internet providers hijacking users' search queries [Online]. *NewScientist*. Available from: http://www.newscientist.com/article/dn20768-us-internet-providers-hijacking-users-search-queries.html#.UuFhuBDFLIV [Accessed 23-01-2014].

Giudice, K. Del. & Gardner, M. 2009. *The Message of the Pensieve: Realizing Memories through the World Wide Web and Virtual Reality.* Unpublished. Available from: http://web.mit.edu/comm-forum/mit6/papers/Delgiudice.pdf.

Govier, T. 1993. Self-Trust, Autonomy, and Self-Esteem. *Hypatia*, 8(1), pp. 99-120.

Greenwald, G. 2014. How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations [Online]. *The Intercept*. Available from: https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/ [Accessed 26-02-2014].

Greenwald, G., Gallagher, R. & Grim, R. 2013. Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'. *Huffington Post*. Available from: http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html [Accessed 07-03-2014].

Griswold v. Connecticut. 1965. 381. U.S. 479.

Guardian. 2009. *Uganda: Unjust and infamous*. Available from: http://www.theguardian.com/commentisfree/2009/dec/05/gay-rights-uganda-wretched-law [Accessed 02-10-2013].

Guardian. 2013. *Product placement* [Online]. Available from: http://www.theguardian.com/media/product-placement [Accessed 23-08-2013].

Guardian US interactive team. 2013. Three degrees of separation: breaking down the NSA's 'hops' surveillance method [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/interactive/2013/oct/28/nsa-files-decoded-hops [Accessed 30-01-2014].

Hare, R.M. 1979. What is wrong with Slavery. *Philosophy and Public Affairs,* 8(2), pp. 103-121.

Hoagland, S. 1988. *Lesbian Ethics: Toward New Value*. Palo Alto: Institute of Lesbian Studies.

Human Right Watch. 2009. *Uganda: 'Anti-Homosexuality' Bill Threatens Liberties and Human Rights Defenders* [Online]. Available from: http://www.hrw.org/news/2009/10/15/uganda-anti-homosexuality-bill-threatens-liberties-and-human-rights-defenders [Accessed 23-08-2013].

Human Rights Watch. 2013. *Laws of Attrition Crackdown on Russia's Civil Society after Putin's Return to the Presidency* [Online]. Available from: http://www.hrw.org/sites/default/files/reports/russia0413_ForUpload_0.pdf [Accessed 13-02-2014].

IAB & IIAC. 2013. *Mobile's Role in a Consumer's Media Day in the United States and in China: The Smartphone as an Extension of the Self and an Extension into the World* [Online].

Available from: http://www.hsph.harvard.edu/nutritionsource/pyramid/ [Accessed 19-09-2013].

Janevic, M.R., McLaughlin, S.J. & Connell, C.M. 2012. Overestimation of physical activity among a nationally representative sample of underactive individuals with diabetes. *Med Care*, 50(5), pp. 441-445.

Johnson, R. 2008. Kant's Moral Philosophy [Online]. *IN:* E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy. Summer 2012*. Available from: http://plato.stanford.edu/archives/sum2012/entries/kant-moral/ [Accessed 10-08-2013].

Kant, I. 1785. Fundamental Principle of the Metaphysic of Morals [Online], translated by Abbott, T.K. *Project Gutenberg* Available from: http://www.gutenberg.org/cache/epub/5682/pg5682.html [Accessed 04-10-2013].

Kant, I. 2003. *Critique of Practical Reason*. Translated by McGregor, M. Cambridge: Cambridge University Press.

Kant, I. 2009. *An Answer to the Question: What is enlightenment?* translated by Nisbet, H.B. London: Penguin Books.

Kramer, A.D.I., Guillory, J.E., & Hancock, J.T. 2014. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS*, 111(24), pp. 8788-8790.

Kymlicka, W. 2002. *Contemporary Political Philosophy: An Introduction.* New York: Oxford University Press.

Lahlou, S. 2011. How can we capture the subject's perspective? an evidence-based approach for the social scientist. *Social science information*, 50 (3-4), pp 607-655.

Leiderman, J. 2013. Justice for the PayPal WikiLeaks protesters: why DDoS is free speech [Online]. *The Guardian.* Available from: http://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech [Accessed 26-02-2014].

Lessig, L. 1999. *Code: And other laws of cyberspace*. New York: Basic Books.

Levin, A. & Striple, G. 2013. *LCV Youth Survey* [Online]. Available from: http://www.lcv.org/issues/polling/recent-polling-on-youth.pdf. [Accessed 19-08-2013].

MacKenzie, D. & Wajcman, J. 1999. *The Social Shaping of Technology*. 2nd ed. Buckingham: Open University Press.

Mann, S. 2002. Sousveillance [Online]. *Wearcam.org.* Available from: http://wearcam.org/sousveillance.htm. [Accessed 05-04-2012].

Mann, S. 2004. "Sousveillance" Inverse Surveillance in Multimedia Imaging. *MULTIMEDIA '04 Proceedings of the 12th annual ACM international conference on Multimedia,* pp. 620-627.

Mann, S. 2012. McVeillance: How McDonaldized surveillance creates a monopoly on sight that chills AR and smartphone development [Online]. *Wearcam.org.* Available from: http://wearcam.org/McVeillance.htm [Accessed 11-12-2013].

Marwick, A. 2013. Silicon Valley Isn't a Meritocracy. And It's Dangerous to Hero-Worship Entrepreneurs [Online]. *Wired.com.* Available from: http://www.wired.com/opinion/2013/11/silicon-valley-isnt-a-meritocracy-and-the-cult-of-the-entrepreneur-holds-people-back/ [Accessed 05-12-2013].

Matyszczyk, C. 2013. Facebook actually sorry for banning breastfeeding pic [Online]. *CNET.* Available from: http://news.cnet.com/8301-17852_3-57578305-71/facebook-actually-sorry-for-banning-breastfeeding-pic/ [Accessed 20-06-2013].

Mill, J.S. 1859. *On Liberty*. London: Penguin.

Moreno, J. 2004. DARPA On Your Mind. *Cerebrum*, 6(4), pp. 92-100.

Morozov, E. 2011. *The net delusion: how not to liberate the world*. London: Allen Lane.

Morozov, E. 2013. The Real Privacy Problem [Online]. *MIT Technology Review*. Available from: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/. [Accessed 05-12-2013].

Murata, K. 2011. The right to forget/be forgotten. In: *CEPE 2011: Crossing Boundaries*.

Nussbaum, M.C. 2003. Capabilities as fundamental entitlements: Sen and Social Justice. *Feminist Economics*, 9(2-3), pp. 33-59.

Nussbaum, M.C. 2007. *Frontiers of Justice*. London & Cambridge: Harvard University Press.

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

O'Hara, K. 2010a. Narcissus to a Man: Lifelogging, Technology and the Normativity of Truth. E. Berry et al., eds. *Second Annual SenseCam Symposium*. Available at: http://eprints.ecs.soton.ac.uk/21904/ [Accessed 20-08-2013].

O'Hara, K. 2010b. Arius in Cyberspace: Digital Companions and the Limits of the Person. In: Yorick Wilks (ed.), *Close Engagements with Artificial Companions: Key social, psychological, ethical and design issues*, Amsterdam: John Benjamins.

Oshana, M.A.L. 2002. The Misguided Marriage of Responsibility and Autonomy. *The Journal of Ethics*, 6(3), pp 261-280.

Pariser, E. 2011. *The Filter Bubble: What the Internet is Hiding From You.* London: Penguin Books.

Parker, E.S., Cahill, L. & McGaugh, J.L. 2006. A Case of Unusual Autobiographical Remembering. *Neurocase: The Neural Basis of Cognition,* 12(1), pp. 35-49.

Patient Protection and Affordable Care Act. 2010. *Public Law 111-148, March 23, 2010.*

Piper, M. 2010. Autonomy: Normative [Online]. *IN:* Fieser, J. & Dowden, B. (eds.). *Internet Encyclopedia of Philosophy*. Summer 2013 Ed. Available from: http://www.iep.utm.edu/aut-norm/#H3 [Accessed 20-08-2013].

Protalinski, E. 2012. Breastfeeding women protest outside Facebook offices [Online]. *ZDNet.* Available from: http://www.zdnet.com/blog/facebook/breastfeeding-women-protest-outside-facebook-offices/8673 [Accessed 10-06-2013].

Putnam, H. 2002. The Collapse of the Fact/value Dichotomy and Other Essays. Harvard University Press.

Quine, W.V.O. 1963. *From a Logical Point of View*. New York: Harper Torchbooks.

Reiman, J.H. 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, *Santa Clara High Tech Law Journal*, 11(1), pp. 27-44.

Rhodes, R. Autonomy, Respect, and Genetic Information Policy: A Reply to Tuija Takala and Matti Häyry. *Journal of Medicine and Philosophy*, 25(1), pp. 114–120.

Rich, M. 2006. Product Placement Deals Make Leap From Film to Books [Online]. *The New York Times.* Available from:
http://www.nytimes.com/2006/06/12/business/media/12book.html?pagewanted=all
[Accessed 10-06-2013].

Rössler, B. 2002. Problems with Autonomy. *Hypatia*, 17(4), pp. 143-162.

Rössler, B. 2010. *Over autonomie en rechtvaardigheid. Oratio 368*. Amsterdam: Vossiuspers UvA.

Saga. 2013. *Lifelogging is better with friends* [Online]. Available from:
http://www.getsaga.com/ [Accessed 23-08-2013].

Sanchez, J. 2013. FBI's Latest Proposal for a Wiretap-Ready Internet Should Be Trashed [Online]. *Wired.com*. Available from: http://www.wired.com/opinion/2013/05/the-fbis-plan-for-a-wiretap-ready-internet-is-misdirected-shortsighted-and-ridiculous/ Accessed 19-05-2013.

Schwartz, P.M. 1999. Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*, 52, pp. 1609-1702.

Sen, A. 2001. *Development as Freedom*. Oxford: Oxford University Press.

Shiffman, J. & Cooke, K. 2013. Exclusive: U.S. directs agents to cover up program used to investigate Americans [Online]. *Reuters*. Available from:
http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 [Accessed 24-05-2014].

Siegrist, J. 2000. Place, social exchange and health: proposed sociological framework. *Social Science & Medicine*, 51(9), pp. 1283-1293.

Stieger, S., Burger, C., Bohn, M. & Voracek, M. Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters. *Cyberpsychology, Behavior, and Social Networking*, 16(9), pp. 629-634.

Taylor, R.S. 2005a. Kantian Personal Autonomy. *Political Theory*, 33(5), pp. 602-628.

Taylor, J.S. 2005b. *Personal Autonomy: New Essays on Personal Autonomy and its Role in Contemporary Moral Philosophy*. Cambridge: Cambridge University Press.

Tate, R. 2010a. Apple's Gay Culture Bans Don't Make it 'Moral' or 'Pure' [Online]. *Gawker*. Available from: http://gawker.com/483486315#comments [Accessed 20-08-2013].

Tate, R. 2010b. Apple Rejects Gay-Sightseeing App Over Gay Sights [Online]. Available from: http://gawker.com/5526475/apple-rejects-gay+sightseeing-app-over-gay-sights [Accessed 20-08-2013].

TED. 2011. *Hasan Elahi: FBI, here I am!* [Online]. Available from: http://www.ted.com/talks/hasan_elahi.html [Accessed 23-05-2012].

Watkinson, C., Sluijs, E.M.F. Van, Sutton, S., Hardeman, W., Corder, K. & Griffin, S.J. 2010. Overestimation of physical activity level is associated with lower BMI: a cross-sectional analysis. *International Journal of Behavioral Nutrition and Physical Activity*, 7(68), pp. 1-9.

Wessler, N.F. 2014. Police Hide Use of Cell Phone Tracker From Courts Because Manufacturer Asked [Online]. *UCLA*. Available from: https://www.aclu.org/blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because [Accessed 09-05-2014].

Yoshida, S., Tanikawa, T., Sakurai, S., Hirose, M. & Narumi, T. 2013. Manipulation of an emotional experience by real-time deformed facial feedback. In: *AH '13 Proceedings of the 4th Augmented Human International Conference*. New York: ACM.

Zetter, K. 2012. FBI Wants Backdoors in Facebook, Skype and Instant Messaging [Online]. *Wired.com*. Available from: http://www.wired.com/threatlevel/2012/05/fbi-seeks-internet-backdoors/ [Accessed 08-01-2013].

6 Beneficence

Introduction

In this chapter the potential harms and benefits of lifelog technology are discussed. The principle that prescribes that one ought to do good and prevent evil is the principle of beneficence (Frankena 1973). Whereas some scholars distinguish between beneficence and non-maleficence as separate principles, such as Beauchamp and Childress (2009) and Ross (2002), in this dissertation beneficence is interpreted as one principle following Frankena (1973) for reasons discussed below.

The chapter follows the same structure as the previous ones. First, the principle is explained in more detail. This explanation includes a normative theory of value. Without an idea of value, one has no instrument to identify harms and benefits, i.e. to promote good and to prevent evil, one will need an idea of what good and evil actually entail. For this inquiry a list containing several goods of intrinsic worth is advanced. The items on the list are identified by Nussbaum (2003) for the Capability Approach (CA). Second, the effect of lifelogs on the good for lifeloggers and non-lifeloggers is discussed. The possible effect of lifelog technology on the items on this list for them can be beneficial or harmful, but could also leave some or all values unaffected. For each capability the challenges and the opportunities are presented. Third, recommendations to guide the optimisation of the ethical desirability with regard to beneficence are presented.

6.1 The principle of beneficence

Historically, some ethical theories have considered the principle of beneficence the ultimate principle that determines moral obligations. One of those theories is utilitarianism as advanced by John Stuart Mill.[115] He considers the promotion of pleasure and the prevention of pain as the main duties of morality (Mill 1863). He states that: "… the foundation of morals, Utility, or the Greatest Happiness Principle, holds that actions are right in proportion as they tend to promote happiness, wrong as they tend to produce the reverse of happiness. By happiness is intended pleasure, and the absence of pain; by unhappiness, pain, and the privation of pleasure" (Mill 1863, 10). According to Mill, there is ultimately only one thing of value, namely happiness in the form of pleasure and the absence of pain. Consequently, all

---

[115] The value he attached to autonomy mentioned in the previous chapter on autonomy (*5.1 Respect for autonomy*) was based on its instrumental use for utility.

obligations and rights are determined and subordinate to this principle. Nonetheless even Mill acknowledges that "some kinds of pleasure are more desirable and more valuable than others" (Mill 1863, 11). If all pleasure would be equally important nothing separates one from "swine" (Mill 1963, 11). In order to make this distinction, there must be other criteria to determine the good besides pleasure.[116] The idea of value will differ from Mill's in important ways. Foremost, the value promoted by Mill, namely 'certain kinds of pleasure', will not be the ultimate value but a list of different goods will be advanced.

Even Immanuel Kant, famously a deontologist, allows some room for beneficence without allowing it to become a strict moral obligation to act (Kant 2002). According to Kant, beneficence belongs to a subset of 'imperfect duties' (Kant 2002). Perfect duties are absolute, and narrowly define the acts that one ought to perform. Controversially, Kant considered it a perfect duty not to lie; it is a duty not to lie even if lying could save the lives of innocent people (Kant 2002). Imperfect duties are primarily duties to adopt a maxim and only indirectly stipulate acts. The duty of beneficence leaves the precise action that one ought to perform in order to act benevolently unspecified; imperfect duties are distinguished by their latitude in application. In contrast to prefect duties, which always constitute a duty to act in a particular fashion, the duty of beneficence prescribes that one ought to adopt a morally obligatory maxim. According to Kant, to promote the ends of others is an end for the individual worthy to adopt but this maxim is not extended to actions, i.e. one is morally free to do more or less towards completing one's duty of beneficence (Kant 2002). In this dissertation, the principle of beneficence is considered a *prima facie* duty, meaning that depending on the context, it can constitute an *actual* duty to act in a particular way.

6.1.1 Beneficence/non-maleficence

The principle of beneficence can be formulated quite broadly as involving four separate duties, namely:

1. "One ought not to inflict evil or harm (what is bad).
2. One ought to prevent evil or harm.
3. One ought to remove evil.
4. One ought to do or promote good" (Frankena 1973).

---

[116] It is out of the scope of this research to address Mill's theory in-depth.

The first duty can also be considered a separate principle, namely that of non-maleficence. For example, Beauchamp and Childress (2009) distinguish between the principle of beneficence and the principle of non-maleficence. According to Beauchamp: "[t]he language of a principle or rule of beneficence refers to a normative statement of a moral obligation to act for the others' benefit, helping them to further their important and legitimate interests, often by preventing or removing possible harms" (Beauchamp 2013) while the principle of non-maleficence prescribes that one ought to refrain from performing acts that harm important and legitimate interests of others. The distinction between the two principles is not made in this study for the three following reasons.

1) The reasons they provide for distinguishing between non-maleficence and beneficence are unsatisfactory. According to Beauchamp and Childress, the principle of non-maleficence prescribes that a certain state of affairs should not come about by one's influence, which often requires the agent to refrain from acting, while the distinct principle of beneficence often requires one to act and subsequently a distinct principle of beneficence is often more demanding than the principle of non-maleficence. Beauchamp and Childress (2009) consider beneficence to require "taking action by *helping* – preventing harm, removing harm, and promoting good – whereas nonmaleficence requires only *intentionally refraining* from actions that cause harm" (Beauchamp & Childers 2009, 151). Elsewhere Beauchamp states that "[r]ules of beneficence are typically more demanding than rules of nonmaleficence, and rules of nonmaleficence are negative prohibitions of action. […] By contrast, rules of beneficence state positive requirements of action" (Beauchamp 2013). Although *often* non-maleficence seems to require no actions from the agent both can, in fact, require positive actions. Indeed, even Beauchamp and Childress mention situations in which non-maleficence requires positive actions, i.e. duties to non-maleficence can also require one to act as to prevent harm: this is the case with negligence in which one has to act in order to ensure that one does not inflict harm (2009, 153) as well as when intentionally withholding or withdrawing treatment in which one has to establish the moral and legal right to do so (20009, 176). In these situations, the duties arising from non-maleficence can demand actions that require considerable time and effort. One issue is that ensuring that one is not in practice harming anyone can require effort. Quite regularly the consequences of one's actions might be unclear and the principle of non-maleficence would require one to become better informed as to prevent one from doing harm. Therefore the moral distinction advanced by Beauchamp and Childress does not hold on this ground.

191

2) Beauchamp and Childress (2009) consider that the principle of beneficence does not have to be always followed impartially and can, consequently, weigh more heavily towards some people than others – although they leave some space for actions that pose little burdens - while non-maleficence weighs equally for anyone (Beauchamp & Childress 2009). According to them, one should help and benefit people based on the relationship one has with them, e.g. one has duties to benefit one's family that one would not have to strangers. The principle of beneficence as formulated by Beauchamp and Childress has been claimed to be outside the domain of ordinary morality (Gert, Culver & Danner Clouser 2006). Beneficence might be commendable but ultimately supererogatory, i.e. it does not provide a duty to act. One of their objections is that Beauchamp and Childress' interpretation of beneficence fails to pass the test of generality as it does not apply equally to everyone, which is a valid objection. However, the weight Beauchamp and Childress provide to relationships is an unnecessary complication to their theory. The underlying concern that beneficence becomes too burdensome without attaching some importance to special relationships is unfounded. The deployment of multiple principles prevents the principle of beneficence becoming too burdensome, as other principles might outweigh beneficence. Indeed the underlying assumption made by Beauchamp and Childress (2009) that the principle of beneficence itself also informs the division of harms and benefits by attaching weight to special relationships seems to supersede and undermine the principle of justice which seems to be traditionally concerned with determining the placement of benefits and harms. There is no need to add a clause that beneficence allows for partiality as made by Beauchamp and Childress (2009) and without such a condition the objection against beneficence made by Gert, Culver and Danner Clouser (2006) is avoided.[117]

3) There is a third reason not to distinguish between beneficence and non-maleficence. Minor infractions of the good might be acceptable when there are gains that outweigh the infringements. As will be shown in this chapter, lifelog technology can harm as well as benefit lifeloggers and non-lifeloggers. Actions can often both harm as well as promote some aspect of the good. For example, if one can save a stranger's life by stopping

---

[117] Besides the reasons discussed above, Beauchamp and Childress advance a third argument. The third argument is that, according to Beauchamp and Childress (2009, 199), non-maleficence provides moral reasons for legal prohibitions for conduct while beneficence usually does not. However this seems hardly a strong moral reason to separate the two principles. Furthermore it is unclear exactly how a single principle of beneficence would preclude legal prohibitions. Lastly, even they hold that this is "generally" (Beauchamp and Childress 2009, 199) the case, which makes the distinction a rule of thumb rather than a strong argument to separate the principles.

him from crossing the street then it is allowed to cause him minor inconvenience by strongly pulling him back. Ultimately the balance of good over evil is decisive in such cases. Therefore, a single principle of beneficence seems more appropriate.

6.1.2 Value

A concept of value is needed in order to identify what constitutes harms and benefits, i.e. what value(s) are ethically relevant when discussing beneficence.

There are different interpretations of the good, without aiming to be exhaustive, three of them will be discussed below. The hedonistic interpretation (which is common) defines the good as happiness but these accounts are unsuitable for this discussion. The effect of a technology on (the amount of) pleasure is complicated to measure as mental states are often non-measurable, but the measuring becomes especially troublesome when one has to examine a point in the future, which is the case for this inquiry. Also, hedonistic accounts fail to include some values, which one commonly would consider valuable in and of itself, such as authenticity (Nozick 1974). There are also theories that consider the fulfilment of desires instead of pleasure as morally good. However, these seem to suffer from the fact that they reverse the way one values the good, i.e. one desires things because they are good and things are not good because one desires them (Crisp 2013).

Instead of defining the good either as pleasure or desire, in this study human capabilities constitute the good. The list advanced is from Nussbaum's interpretation of the CA:

1. Life. Being able to live to the end of a human life of normal length; not dying prematurely, or before one's life is so reduced as to be not worth living.

2. Bodily Health. Being able to have good health, including reproductive health; to be adequately nourished; to have adequate shelter.

3. Bodily Integrity. Being able to move freely from place to place; to be secure against violent assault, including sexual assault and domestic violence; having opportunities for sexual satisfaction and for choice in matters of reproduction.

4. Senses, Imagination, and Thought. Being able to use the senses, to imagine, think, and reason and to do these things in a "truly human" way, a way informed and cultivated by an adequate education, including, but by no means limited to, literacy and basic mathematical and scientific training. Being able to use imagination and thought in connection with experiencing and producing

works and events of one's own choice, religious, literary, musical, and so forth. Being able to use one's mind in ways protected by guarantees of freedom of expression with respect to both political and artistic speech, and freedom of religious exercise. Being able to have pleasurable experiences and to avoid non-beneficial pain.

5. Emotions. Being able to have attachments to things and people outside ourselves; to love those who love and care for us, to grieve at their absence; in general, to love, to grieve, to experience longing, gratitude, and justified anger. Not having one's emotional development blighted by fear and anxiety. (Supporting this capability means supporting forms of human association that can be shown to be crucial in their development.)

6. Practical Reason. Being able to form a conception of the good and to engage in critical reflection about the planning of one's life. (This entails protection for the liberty of conscience and religious observance.)

7. Affiliation.

A. Being able to live with and toward others, to recognize and show concern for other human beings, to engage in various forms of social interaction; to be able to imagine the situation of another. (Protecting this capability means protecting institutions that constitute and nourish such forms of affiliation, and also protecting the freedom of assembly and political speech.)

B. Having the social bases of self-respect and non-humiliation; being able to be treated as a dignified being whose worth is equal to that of others. This entails provisions of non-discrimination on the basis of race, sex, sexual orientation, ethnicity, caste, religion, national origin.

8. Other Species. Being able to live with concern for and in relation to animals, plants, and the world of nature.

9. Play. Being able to laugh, to play, to enjoy recreational activities.

10. Control over one's Environment.

A. Political. Being able to participate effectively in political choices that govern one's life; having the right of political participation, protections of free speech and association.

B. Material. Being able to hold property (both land and movable goods), and having property rights on an equal basis with others; having the right to seek employment on an equal basis with others; having the freedom from unwarranted search and seizure. In work, being able to work as

a human being, exercising practical reason and entering into meaningful relationships of mutual recognition with other workers (Nussbaum 2003, 41-42).

In its original form the list is used as part of a political theory of justice and a reaction to the exclusive focus on resources in policy.[118] Here it will be used as a normative theory of the good. The list of capabilities has a different function within the CA than it has here. In the CA freedom was the ultimate value that needed to be promoted. For example, the second capability, bodily health, implies that one needs to have the opportunity to eat healthily. Consider the difference between fasting and famine (Sen 2001, 76). Both can cause starvation but there is an important difference between them, namely fasting is the result of a choice. According to the CA, one should be able to eat healthily, but the choice to actually have a healthy diet should be left to the individual. This way, people are not forced to live a particular conception of the good life.[119] The capabilities are part of a "thick vague conception of the good" (Nussbaum 1997, 277) which is compatible with reasonably and deeply held cultural and religious beliefs. Nussbaum wants to allow the individual to live well according to their values and beliefs provided that these are reasonable. Having these capabilities allows people the necessary opportunities to give form to such a life.

---

[118] The origins of the CA and application of it are actually quite illuminating for the functioning and aim of the theory. Amartya Sen has been credited as the founder of the CA. It has been developed as an instrument to influence policy and has been quite influential in achieving its aim. For one, the United Nation Development Program Human Development Report bears the mark of it (Fukuda-Parr 2003, Robeyns 2006). The common practice to measure the development of a country primarily with GDP based standards is rejected when using the CA. The GDP per capita can conceal the poor level of opportunities marginalised groups deal with. There is no causality between the GDP per capita and access to healthcare, life expectancy, or education. Illustrative is the mortality rate of the African American community in the United States of America. Afro-American men have a higher mortality rate than their Chinese, Sri Lankan, Jamaican and Costa Rican counterparts (Sen 2001, 96). Another approach, to judge freedom *merely* on procedures, such as a free market democracy in which citizens enjoy passive and active suffrage, is also rejected by the CA (Sen 2001, 17). The critical indicator of the opportunities of a person is neither provided by GDP standards nor by democratic procedures alone. To provide a better insight into the opportunities of persons, he proposes an approach which does justice to the myriad of factors that constitute the possibilities of an individual to shape its life. Unfortunately, Sen offers no list whilst they are advantages to having it as it can be an instrument to distinguish between desirable and undesirable opportunities. The desirability of some capacities is clearly debatable (Nussbaum 2003). After all, an intrinsic property of freedom is that it is comes with constraints; the freedom of A to do x accompanies the restriction of B not to interfere with x (Nussbaum 2003, 44). For example, the freedom of a woman to protect her bodily integrity inevitably leads to other people being constraint to violate her bodily integrity. Therefore, the freedom of a man to have intercourse with his wife without her consent is to be restricted, which limits hers but advances his opportunities.

[119] Contrary to other theories of justice, most notably Rawls', the CA entails that a fair distribution is based on opportunities instead of resources. Resources can be grossly inadequate to determine the opportunities one has (Nussbaum 2007, 74). Rawls' concept of 'basic goods' however is too narrow to be an effective instrument to provide people with the means to live a life worthy of dignity because it puts too much of an emphasis on income and wealth.

In this dissertation, instead of focusing on choice, which Nussbaum does, the capabilities are considered aspects of the good. For example, the capability 'play', according to Nussbaum, amounts to ensuring that an individual has sufficient opportunities for leisure and other things related to 'play'. Societal or political pressure that forces people to enjoy some free time – for example legal holidays which are mandatory while one may prefer to work – would be undesirable as it would take away people's choice following Nussbaum. However, in this study, such advancements of 'play' would be considered desirable as it would advance an aspect of the good provided that it provides a greater balance of good over evil. Instead of focusing on someone's choice, which should be the focal point according to Nussbaum's interpretation, the actual fulfilment of the capability becomes imperative. Let's consider another capability, namely 'bodily health'. In case that lifelogs successfully become a leading cause for social pressure on lifeloggers and non-lifeloggers to live healthier, then this is considered an advantage of lifelog technology. For the CA as interpreted by Nussbaum, the pressure exerted on people to use lifelogs to improve their lives hinders choice and should be considered undesirable.[120]

Scholars have already argued that Nussbaum unintentionally promotes a particular conception of the good. Deneulin (2002) has argued forcefully that the CA cannot be neutral on how people should live. One of her arguments is that Nussbaum maintains that any reasonable person can endorse the capabilities as essential for them to live a worthy life regardless of that person's specific conception of the good. If this is the case, then surely these capabilities are essential to the good. Another argument made by Deneulin is that the focus on choice alone is often inadequate to provide people with the capabilities (Deneulin 2002). She mentions the interdependencies that exist between people and capabilities in order for people to enjoy these capabilities. Deneulin elucidates this by mentioning environmental problems. According to Nussbaum, one should be free to choose to live in an unpolluted environment, e.g. her interpretation makes no difference between dumping rubbish on the street and disposing garbage responsibly. Following Nussbaum's interpretation, the CA addresses choice and is agnostic regarding the good. However, the rubbish thrown on the streets by one impedes the choice of others to live in an unpolluted environment. The opportunity to live in a clean environment often requires measures that prevent people from

---

[120] In this study, concerns about people having too little freedom to give form to their own lives can be accounted for. Beneficence does not necessarily outweigh concerns for autonomy. By deploying a normative framework in which there are different values and principles at play, one can prevent beneficence or a single capability from becoming too dominant.

polluting. Only when one considers the capability worthy of pursuit and, consequently, restricts people's opportunities to pollute, is this capability feasible. Also the opportunities people have are dependent on their actions according to Deneulin (2002). Without health one may lack many other capabilities. Nussbaum endorses this position and considers health and bodily integrity as so essential to other capabilities that sometimes intervention in people's choice is warranted when they fail to take sufficient care for their health (Nussbaum 2000). However, this seems a paternalistic intervention which seems at odds with her idea that people should be free whether to actually use the freedom they have available to them. After all one decides for that person that health is more important than he valued it to be. There seems no reason why this would not apply to other capabilities if the failure is so sever that it jeopardises other capabilities. Hence Nussbaum allows interference when the good is considered too important for people to be risked. Again this shows that she implicitly deploys a conception of the good.

6.1.3 Justification for the use of the principle

Beneficence is not a fringe principle within ethical theory but has been widely considered as important in the tradition of normative ethics in the Western world. The weight attached to beneficence within this research is not controversial.

The place that beneficence can have in deontological theory is already discussed by explaining briefly the theories of Kant and Ross. In fact, this chapter and dissertation is an example that the principle of beneficence can be important within deontological thought.

The brief discussion on Mill showed that the principle of beneficence is closely related to utilitarian theory in which the greatest balance of good over evil is paramount.

The third of the major strands of normative ethics in the Western world is virtue ethics and also in virtue ethics the promotion of the good has a prominent place. 'Benevolence', in other words, having the disposition to act for the benefit of others, is considered a morally desirable character trait. According to Aristotle virtuous activities mean living well (Aristotle 1998). *Eudaimonia*, which roughly translates to 'human flourishing', 'happiness' or 'well-being' constitutes for Aristotle the highest good. In order to live a virtuous life one needs practical wisdom and particular goods such as friendship, wealth, and power. Nussbaum actually refers to the Aristotelian notion of 'human flourishing' but she allows pluralistic conceptions of the good (Nussbaum 2007, 182, 190) while Aristotle had one particular

interpretation of the good life. She interprets this as allowing the individual to live well according to their values and beliefs provided that these are reasonable.

6.2 Challenges to and opportunities for the capabilities

In the next part, the effect of lifelogs on the various capabilities is discussed. The structure is as follows: the capabilities are discussed one by one following the order of the list presented above. Some individual capabilities consist of multiple and diverging parts and, when appropriate, these parts are discussed separately. For each capability or part of a capability the challenges (issues with the technology that need to be solved) and opportunities (advantages of the technology that can be reaped) are discussed separately so it becomes immediately clear where the challenges and opportunities lie. These discussions are concluded with an overall assessment of the effect of lifelogs on the whole capability to clarify if the effect expected of lifelogs is largely positive or negative. This section is concluded with a summary in which the overall effect of lifelogs on beneficence is discussed.

6.2.1 Life

"Life. Being able to live to the end of a human life of normal length; not dying prematurely, or before one's life is so reduced as to be not worth living" (Nussbaum 2003, 41).

Challenges: The capability 'life' seems to remain largely unaffected as this kind of technology is often considered to have little effect on one's life expectancy. Technological devices in some of the most important target markets for technology, such as the EU and the US, are subject to rules and regulations to protect the health and safety of consumers. Presumably the devices that are developed for the EU or the US will also be used for other markets and these markets would, for that reason, also enjoy technology that is not dangerous. In addition, if these devices would be unsafe then it seems very unlikely that they would be attractive to the vast majority of consumers. There are however three minor remarks to make.

1) One apparent issue regarding safety is that information could be delivered in an untimely manner. Imagine receiving information from a lifelog application on one's lenses or through one's glasses. The fact that information is directly projected on one's field of vision might distract. This can prove dangerous in some contexts, such as when driving or cycling. However, lifelogs are by no means the sole providers of such information, as one might also receive text messages, news updates, chats, or emails. Moreover, it mainly is the platform

that offers this information that is of concern. Prompts are not an intrinsic feature of lifelogs and can easily be avoided. Already some mobile phones have a 'Driving Mode' that limits the functionality of a smartphone so drivers are not disturbed. A similar measure could be used for prompts from lifelogs.

2) Both Van den Hoven (2008) and Nissenbaum (2004) mention cases in which a murderer or stalker tracked the whereabouts of their victim through publicly available resources, such as the murder of actress Rebecca Schaeffer in 1989 and that of Amy Lynn Boyer in 1999. In both cases the murderer could trace its victim through publicly available information. Van den Hoven (2008) also mentions the crimes committed by the Nazis in the Second World War against the Jews to show that personal information could be used to violate international law and human rights. Nonetheless, it seems questionable if lifelogs are the most opportune source of information to trace people. After all, the previously mentioned murders took place before the advent of technology such as lifelogs. Indeed, in recent times a vast amount of sources have become publicly available which do not require the hacking into private accounts.

3) A final issue is that the information obtained through lifelogs could be used to bully persons. The increased ability to anonymously contact specific individuals and share digital information covertly facilitates ominous harassment. In the worst case, suicide is linked to the spread of information and digital harassment.[121] However bullying seems the result of communication technology such as social networking sites rather than sources creating personal information such as lifelogs. Moreover, if lifelogs are secure and do not capture information about others, then the only information which can be used to bully would come from lifeloggers sharing personal information about themselves, making the sharers at least partly responsible.

Conclusion: Lifelogs might have a minor negative effect on the capability 'life'. However, the negative effect is likely to occur only sporadically.

6.2.2 Bodily Health

"Bodily Health. Being able to have good health, including reproductive health; to be adequately nourished; to have adequate shelter" (Nussbaum 2003, 41).

---

[121] There have been high profile cases of adolescents committing suicide because of digital bullying (Guardian 2013; Henley 2013).

Lifelogs are unlikely to have an effect on having adequate shelter but lifelogs can promote as well as harm certain aspects of health. First the opportunities lifelogs offer to promote health are discussed. Second the challenges posed by lifelogs to health are discussed.

Opportunities: Lifelogs can offer information relevant to health that can be used by either the lifelogger or third parties to improve health. Most of the benefits are related to the fact that lifelogs can create an unprecedented amount of personal information relevant to health and distribute this information with little effort or resources required. By doing so lifelogs could improve (1) the health of the lifelogger and others, and (2) medical care.

1) Lifelogs can both create a greater understanding about health and healthy behaviour but also create an environment in which healthy behaviour is encouraged.

Lifelogs could become a tool to improve the health of the lifelogger. Some diseases can be prevented by adjustments of lifestyle, such as non-communicable diseases (see also *3.2.2.4 Health benefits*). These diseases include heart disease, stroke, cancer, diabetes, and obesity and form a heavy burden on the sufferers, their family, and society at large. Lifelogs might be especially useful when they can simplify information about nutrition. Diets are complicated to track, while the labelling of food products and their nutritional value is often difficult to understand. A lifelog that can show the lifelogger shortcomings and excess in their diet, in conjunction with measuring biomarkers to customise recommendations for diets, can be extremely beneficial for health. There is evidence that tracking health indicators can improve health (Fox & Duggan 2013). Another advantage is that lifelogs can capture information that is difficult to be captured through other means than technological devices, such as information about one's sleeping patterns, which could be used to address potential issues with sleep. Addressing sleeping problems is important as these problems are associated with poor prognosis for people at risk for cardiovascular disease and strokes (Dement & Mitler 1993).

Partly due to the rise of non-communicable diseases and partly due to an ageing population there is concern for the affordability and staffing of healthcare (World Health Organization 2011). Lifelog devices might be able to perform some of the tasks of healthcare professionals *and* they might be able to perform these tasks more regularly and more inexpensively. Lifelog devices can monitor a person nonstop throughout the day without requiring a clinical environment, and the additional costs of such a clinical environment, with low-cost equipment. Already there are cases of people improving their health by using

wearable devices. Larry Smarr, director of the California Institute for Telecommunications and Information Technology has prided himself on being a pioneer in improving lifestyle by capturing as much data as possible relevant to health (Cohen 2012).[122] With the help of these trackers his weight dropped from 205 to 184 pounds. He uses this method not only to lose weight - there are more straightforward ways to achieve a 20 pound weight loss - but also to prevent further issues with his health. For preventive purposes he decided on the use of a hundred biomarkers to track the effect of his diet on his health. An analysis of the results of these biomarkers allowed him to outwit the doctors when he signalled a disease well before he experienced any symptoms. Early diagnosing can prevent costly and invasive procedures at later stages. Even without the use of a hundred biomarkers, lifelogs could allow a better understanding of health. 'Simple' devices such as pedometers and heart rate monitors providing information about stress levels and physical activity can improve understanding about health-related behaviour. For example, one often overestimates one's exercise, which can negatively impact health (Janevic, McLaughlin & Connell 2012; Watkinson et al. 2010). Because the devices and sensors are often already integrated into daily life or become increasingly part of daily life there is no additional inconvenience associated with wearing or carrying these devices.

The insights gained and the improvements made through lifelog technology can also positively affect others. The insight gained by the lifelogger might also benefit others as the lifelogger does not live in complete solitude. Lifeloggers might begin to advise others using insights obtained from lifelog technology. Also, a lifestyle change by the lifelogger will most likely affect those close to the lifelogger. Lifelogs can be beneficial to improve one's diet and one person changing their diet in the household can lead to everyone having different dinners.

Lifelogs for health might even increase the pressure exerted on people to live healthier. The usefulness of lifelogs for health can require people to take greater responsibility for their health. To assign responsibility, actions and their consequences have to be in some way intended and informed. Assigning responsibility is not merely a statement

---

[122] Smarr is not considered a lifelogger but a 'quantified-selfer'. The Quantified-Self is basically a movement of which its members gather quantifiable information about their lives. One of the main differences between quantified-self and lifelogging is that the information retrieved is presented in numbers (steps taken in a day, the number of friends one has met, blood pressure, amount of emails sent/received, etc.) while the lifelogger could also be presented with qualitative information (photos, content of emails, etc.). Data from the Quantified-Self movement could be part of the lifelog while some information from lifelogs (such as the data above) are not part of the quantified-self.

about causality. The act of holding someone responsible is also a normative statement about one's duties. To hold a person morally responsible for her deeds (or her inactivity) is to assign blame or praise stating that she ought to have acted differently or was correct in acting as she did (Frankena 1973). With the advent of lifelogs for health it would become less convincing to argue that one was unaware of the consequences of particular behaviour for health and that the harms to health were unintended. People could become more vulnerable to accusations of negligence or imprudence. People could actively pursue being praised or punished and create social communities. Social platforms may be purposely used by people to share data and inspire each other to become healthier. One can think of online forums in which members can anonymously distribute information.

2) Lifelog applications might also be designed to provide useful information to carers or policy-makers. The trove of information gathered by lifelogs might be used by carers to improve healthcare for the lifelogger. After all, the amount of data gathered by lifeloggers could allow an unprecedented personalisation of therapy or other treatments.[123]

Lifelogs could be used to gather information that was burdensome to obtain before the advent of lifelog technology. An overview of one's diet, which is notoriously difficult to gain for others, can be shared immediately with the physician, coach, or therapist with little to no effort (O'Hara, Tuffield & Shadbolt 2009). One can improve diagnoses and therapy by providing more and more exact information about the behaviour and the mental and physical condition of the lifelogger and the impact of the therapy and treatment (Allen 2008; Bell & Gemmell 2009; O'Hara, Tuffield & Shadbolt 2009). Indeed, by virtue of lifelogs one may even be able to adjust doses and therapy to the individual preventing waste and improving care. The alleviations in distribution of personal information also allow the spread of medical care to places that are difficult to access by physicians or medical staff. Lifelog technology might also be made to support telemedicine to provide healthcare at a distance allowing care for remote areas or to patients having trouble accessing care.[124]

Another use for lifelogs might be preventive monitoring. For instance, one's domestic energy consumption can explain a lot about one's lifestyle and can therefore be made suitable for carers to ensure that people are maintaining their lifestyle (Smeaton 2011). Such

---

[123] There are also more indirect effects on health by lifelogs. Below is discussed (*Other Species*) how lifelogs could improve the environment which has obvious advantages for health.

[124] Tele-medicine is not without its own ethical issues, such as trust, the missing human element to care, and responsibility.

applications could be especially useful to assist carers for people with diseases such as dementia, whose condition is progressively getting worse. Deviations from one's daily routine could be a sign that one's situation is deteriorating. Lifelogs might allow the monitoring outside a clinical environment possibly prolonging the time before the person needs to be admitted to a nursing home.

Lifelogs could even function as one's medical record in which one can store information about previous medical procedures and medicines. This would have the further advantage that it may not be the health system that possesses one's medical record but the patient. In the latter case the lifelogger should have the lifelog stored on a personal server rather than in a cloud or other corporate server. The lifelogger possessing his record would take away at least one of the privacy issues associated with digital medical records, namely that others possess and can distribute the data.[125]

Lifelogs could be useful to discover new trends and correlations with regard to health. The collection of data from multiple lifelogs could provide general insights into the health and lifestyles of populations. Lifelogs might become an incredible source to monitor epidemics and prevent or repress them (O'Hara, Tuffield & Shadbolt 2009). Already, the spread of the flu can be monitored by using social networks as Twitter that share text and GPS coordinates (Sadilek, Kautz & Silenzio 2012). When lifelog data would be aggregated, the potential to discover new correlations would be unprecedented, e.g. if a significant number of people in a certain geographical area all come down with the same type of cancer or disease, it could help doctors determine the cause, the reason why some people are more susceptible than others, or even just identify the pattern. The collection of data from lifelogs of different people could facilitate research by harvesting and digitally querying unprecedented amounts of data of an unprecedented number of people taken into account the numerous potential variables with the immense computational power of technological devices.

Even outside the realm of medicine or care the existence of data can be beneficial. Policy-makers might obtain a better insight into health and healthcare by obtaining access to anonymous and aggregated data from the lifelogs. These insights could even be obtained through opt-in procedures allowing participants a choice about their privacy.

---

[125] However personal storage creates other issues. The burden of protecting privacy is now placed with a person who may not be competent enough either to foresee the consequences of sharing his data or to secure the lifelog against third party access.

Challenges: As mentioned in the literature review (*3.2.1.7 Psychological and health risks*), there are also potential challenges to health. These challenges comprise both challenges lifelog technology poses directly to health and obstacles that need to be overcome to make lifelog technology appropriate for the purposes of improving health.

1) Lifelogs might be unsuitable to sufferers from mental illnesses. Although, wearable lifelog devices such as the SenseCam – a wearable, automatic lifelog camera - can be useful to treat depression (Murphy et al. 2011) it is also possible that sufferers from mental disorders or pathologies outside clinical environments have their conditions aggravated by lifelogs. As mentioned above (*3.2.1.7 Psychological and health risks*), lifelogs were identified as a potential risk to sufferers from bipolar and unipolar depression (Allen 2008; Rawassizadeh & Min Tjoa 2010; Rawassizadeh 2011) presumably because lifelog technology allows uncontrolled and unconstrained retrieval of information from the past. Lifelogs maybe function as a constant (and recorded) reminder of the current lifestyle they are now or were living, which they most likely do not view as ideal, which may, in turn, perpetuate the cycle of depression and make them feel worse. One might make the same case for people with anxiety disorders. A symptom of the disorder is becoming overly concerned with quotidian matters, and it is not hard to imagine that keeping a lifelogging device could exacerbate this. Above it was mentioned that information about healthy behaviour could be shared within online communities in which healthy behaviour is encouraged. However, the opposite could happen as well. Sufferers from anorexia, who in general are strongly vulnerable to influences from their social community (Brotsky & Giles 2007), could share recording of their unhealthy behaviour as stimulants for others.[126] Moreover, the recalling of an event can be emotionally harmful, for example, when a memory is evoked about an event that led to a post-traumatic stress disorder (Allen 2008).

Lifelogs indeed seem to be unsuitable for people with particular kinds of mental health issues, and if the use of lifelogs does indeed prove harmful the use of these devices by them should be discouraged. This seems only possible when the groups to whom lifelogs are harmful are well-defined and one can specifically mention the pathologies and disorders for which lifelogs are unsuited.

---

[126] However, this community is notoriously secretive. Information obtained from lifelogs about their behaviour might be very valuable.

2) There might also be issues with lifelogs negatively affecting biological memory. Some mention cognitive laziness (Del Giudice & Gardner 2009): people will not use their own memory but rather rely on their lifelogs. Nicholas Carr (2010) has been cautionary about the effect of the Internet on people's mental abilities. According to him, the Internet is actually harming people's mental skills. When parts of the brain are left unused they might lose their functionality, in other words, atrophy might occur. This way, an artificial memory is not necessarily an enhancement of the brain, because it could possibly reduce biological memory (Murata 2011).[127] This issue seems overstated for lifelogs. The occurrence of atrophy depends on persons favouring the lifelog instead of consulting their biological memory; however, it seems likely that often the use of lifelogs would require more effort than the use of one's memory, which is readily available without needing additional actions, such as tasking a lifelog. Also at times one may prefer to reminisce about the past rather than to obtain a factual account of the past (O'Hara 2010; Chen & Jones 2012). Moreover, the fact that lifelogs will fail to capture everything (correctly) will often render them insufficient requiring the use of biological memory or social interaction; one cannot rely solely on lifelog information. Indeed, lifelog data function as mnemonics offering clues rather than memories (Sellen et al. 2007). Often one will need to use one's memory to complement or correct the data. In addition, studies have indicated that lifelog devices might actually improve certain functions of memory (Finley, Brewer & Benjamin 2011; Silva et al. 2013). Even if lifelogs change neurological paths - the change is by itself not negative *per se* as many inventions and changes in one's environment have done so - it seems far from evident that they will actually reduce biological memory which would be the real issue here.

3) Access to healthcare can be jeopardised when lifelog information is used unjustly. The spread of lifelog information might be used to create risk profiles. Certain character traits, sporting or eating habits, family diseases, visited locations, etc. are or might become indicators to show higher susceptibility for disease or accidents. As a consequence insurers might judge people, whose lifelog shows high risks to health, ineligible for coverage or raise the quotes considerable and so effectively hindering their access to healthcare. The above mentioned fact that people can be increasingly held responsible for their actions might

---

[127] The reduction of biological memory would be undesirable for other reasons than health as well. After all, these reductions would allow people that can manipulate the content an incredible power to influence one's memories of the past as the lifeloggers would be unable to correct this information using their biological memory

aggravate this issue. Society or governments might mince the usage of lifelog information by insurers because some risks to health are seen as a result of imprudence or negligence, such as having an unhealthy diet or smoking. However, as discussed before (*3.3.5 Corporations as actors*), this would allow insurers too much power over the individual. For one, insurers are likely to focus exclusively on matters important to their business model, such as health. However, health is only one aspect of the good and sometimes one accepts trade-offs to health in order to maintain other aspects of the good. By exclusively focusing on health a too narrow account of the good is advanced. In addition, allowing insurers to use this information might mean that one would need to avoid these risks (if that is possible at all) or accept that one's access to healthcare might be at stake. Effectively one's freedom would be curtailed. By providing insurers with lifelog information one will overall be worse off as it poses both a challenge to one's freedom as well as affordable healthcare. Again, this issue is dependent on limiting the use and access of lifelog data by insurers or other parties and it stresses the need for security and privacy

4) In order for lifelogs to improve health they need to offer a sufficient standard for the quality of information suitable to enrich understanding, but this does not need to be the case. Lifelog applications might (in)advertently promote an unhealthy lifestyle because the information they present might be deficient. Based on deficient lifelog information, one might change one's behaviour for the worst. There could also be ulterior motives such as commercial interests for the low quality of content. Lifelogs could be used to promote products or behaviour that is unhealthy. Pharmaceutical companies or producers of consumer goods might benefit from lifelogs promoting aspects of health that would suit their products or they would profit from particular assessment of the healthiness of their product.

Moreover, there may be issues when the device unexpectedly fails to work properly. The placement of responsibility becomes more diffuse.[128] Health could be negatively affected when the devices are unreliable, of low quality, or unsuited for their purposes. If the blurring of boundaries between consumer and medical devices is a trend that is worth further pursuing, then one ought to find ways to ensure there are sufficient checks and balances in

---

[128] Questions can arise such as to what extent one can hold other stakeholders responsible when the lifelogger uses incorrect or incomplete information from the lifelog? The lifelog may fail to provide the correct information for numerous reasons, such as: flaws within the design; broken parts; infringement by third parties; biased information; confusing representation of information; misuse by lifelogger; conflicting information; too much information; etc. When one makes decisions based on information from a lifelog, the issue of assigning responsibility can become more diffuse.

place to warrant the quality and reliability of data. Issues with quality and reliability of data might be alleviated by finding approval of government bodies that should function as a controlling external body such as the US Food and Drug Administration (FDA).

5) In the current environment in which there is no tradition of people bringing their own data to physicians, self-harvested data might prove a burden to healthcare resources and staff. Smarr was capable of separating signal from noise maybe even better than his doctor, who (at first) chose to ignore his data, but one cannot expect everyone to possess the same ability to identify issues. The devices need to be integrated into the daily operation of healthcare, e.g. physicians need to be able to trust the data to use them. Also consumers need to be able to use the devices correctly and should not demand medical assistance without sufficient reason. Lifeloggers, who consult medical experts without there being any medical need because of harmless deviations brought to light by lifelogs, could burden the healthcare system.[129] A correct interpretation by the lifelogger or presentation by the company offering the product of the results of the device is also to the direct benefit of the lifelogger. If the lifelogger or the device fails to properly distinguish between signal and noise, then one might start perceiving irrelevant deviations as significant which could cause anxiety to the lifelogger and her environment. In addition, self-testing by lifeloggers could cause anxiety, e.g. when healthcare professionals do not accept or dismiss the findings of the device, when there is no medical solution to the identified abnormality, or when the lifelogger has no access to healthcare facilities (Scott 2014).

6) Another issue is that lifelogs could be ineffective altogether when they fail to motivate the lifelogger to actually improve their health (or other behaviour for that matter). Information by itself can be insufficient a motivator to change behaviour. After all, despite knowing that some acts have negative repercussions, people at times fail to adjust their behaviour. Social equality and self-esteem seem to be other factors that play a part besides understanding the effect of particular behaviour (Marmot 2013; Siegrist 2000). In addition, the technology may fail to reach the target market that would profit most. Also others, who can profit from these devices such as the elderly, the infirm and persons suffering from chronic illness, seem to be amongst the ones that can profit most but do not seem to use devices often. One study found that 70-80% of people with a chronic condition kept some of record about some health indicator and 72% said that keeping score had an impact on their

---

[129] In the case that rough indications are sufficient, data from applications might be already accepted such as applications keeping track of one steps or one's menstrual cycle.

healthcare routine (Fox et al. 2013). Out of these people, 41% uses pen and paper and 43% use their memory to track these conditions. Only 4% uses an application or another tool on their smart phones. Moreover, devices can fail to keep the consumer interested; there is research that indicates that more than half of the users of wearable fitness tracking devices stop using them within half a year (Ledger & McCaffrey 2014). One step to increase the effectivity of lifelogs is to create an inclusive design adjusted to accommodate users from diverse socio-economic and cultural backgrounds. Moreover, lifelogs might be designed to allow the users to set goals or share their achievements and by doing so create communities in which healthy behaviour is encouraged.

7) The previously mentioned shortcomings of lifelogs to capture all aspects of the lifelogger's life (*5.2.1.1 Biases*) can lead to a narrow understanding of the self that fails to include, amongst others, all that is of intrinsic worth. One such issue is medicalisation. Tracking bodily signals might lead to the medicalisation of the human body, i.e. it might make anything supervenient to concepts of health and illness. Kukla and Wayne (2011) provide three negative consequences related to this issue. One of the negative side effects of it is that one can hold oneself increasingly responsible for one's health and behaviour ignoring other aspects of life. Taking care of one's health might become too great a burden. Additionally, it might increase the dependency on devices: one can be held increasingly responsible for things one needs devices for, so one increasingly needs to use these devices to avoid being blamed. Furthermore, by attaching weight to devices, the weight to personally held intuitions might be diminished. Only conditions lifelogs capture might be relevant and self-experienced indications might be ignored if they fail to be supported within a lifelog. Society can also be 'medicalised' by governmental bodies or corporations who start assessing and regulating behaviour primarily based on increased insights about health and illness (and their costs) obtained from lifelog data while failing to attach proper weight to other aspects of the good. Issues with medicalisation might be avoided. Lifelogs might also capture information about other aspects of the good namely the environment or one's social life. Indeed, the fact that lifelogs can be used for many other aspects makes it less likely that issues with health and illness become too dominant.[130]

Conclusion: In general, lifelogs seem an instrument that can be used to promote health, although there are still many challenges that need to be accounted for before lifelogs

---

[130] Instead of medicalisation the person could become increasingly judged on digital information.

can become an effective tool to improve bodily health. Most of the challenges posed by lifelogs are practical and concern the quality and reliability of information and their motivational force, except for the issues of neurological changes and medicalisation. The effect on lifelog technology for neurological changes is yet far from clear, while the risk for medicalisation is reduced when lifelogs offer persons information suitable for other purposes as well.

6.2.3 Bodily Integrity

"Being able to move freely from place to place; to be secure against violent assault, including sexual assault and domestic violence; having opportunities for sexual satisfaction and for choice in matters of reproduction" (Nussbaum 2003, 41).

The effects of lifelogs on bodily integrity are ambiguous. The opportunities will be discussed first.

Opportunities: Lifelog technology could help protecting the bodily integrity of its users. The need for better protection against assault is vast, creating an urgent need for technology to protect people. According to Heise, Ellsberg and Gottemoeller (1999), at least one in three women, roughly one billion, have been physically, sexually assaulted, or otherwise abused.[131] Of all violent crimes, 25% are committed by a man against their partner (Women's Aid 2013). Meanwhile there is a need for more evidence as one in every three rape allegations in the UK do not make it past the investigation phase due to evidence issues or victim credibility (Cybulska 2007). This violence happens behind closed doors and is barely visible to outsiders as households are allowed a significant degree of privacy. The use of wearable devices that capture audio and visuals are obvious deterrents for assailants (Allen 2008; Brin 1998) but even when lifelogs do not deter persons from assault, the information might be useful as evidence to incriminate the attackers creating a safer environment to those vulnerable to assault. Lifelogs can capture information that can indicate malice and/or provide circumstantial evidence such as lifelogs that can capture unusual high levels of stress or other body signals. A person contemplating sexual assault might be dissuaded from committing the attack when he realises that he is being recorded or that the lifelogger might have evidence that points to malice.[132] Moreover, the lifelog might even inform lifeloggers

---

[131] Other forms of abuse are economic and psychological abuse.
[132] This will become even more relevant when identification techniques improve and people are increasingly able to identify people based on soft biometrics such as gait.

about ways to protect themselves in surprising ways. Gunns, Johnston and Hudson (2002) discovered that the manner in which one walks is an indicator of one's likelihood to being assaulted. Similar to lifelogs giving feedback about posture to improve health, lifelogs might be able to inform the lifelogger about posture to protect one's bodily integrity.

Challenges: Lifelogs can also affect bodily integrity negatively. Many of them stem from a failure to protect privacy. The following three issues with bodily integrity are mentioned below: (1) harm to intimacy, (2) embarrassment and humiliation, and (3) reduction of freedom regarding matters relevant to the protection of bodily integrity.

1) The lack of privacy potentially caused by lifelogs might harm intimacy. Gerstein defines intimacy as being so completely immersed in an experience that it forms a person's "consciousness and action" (Gerstein 1978, 77). Being monitored distracts. It makes people assume the perspective of the observer. The threat or awareness of being observed and possibly judged by others creates a different relation to the moment than when being engrossed in something in solitude. The lack of intimacy might harm the establishment and maintenance of relationships. With a wide proliferation of lifelog technology that capture information about others it would be imprudent to immerse oneself without taking into consideration that someone might be recording. Lifelogging devices might be camouflaged or for other reasons barely visible making it risky to reveal oneself in the most literal sense. For prudential reasons it might be advisable to avoid intimacy when one is uncertain about the presence of lifelogging devices capturing audio or video.

Interestingly enough those behind the development of Autographer, a wearable camera that takes pictures automatically, seem to acknowledge the fact that recording devices can disturb intimacy albeit in another way than discussed above. According to the company lifelog devices are a solution to issues with intimacy rather than a problem as they state: "[w]hy live these precious moments through a lens? Autographer captures the memories for you, as they happen, with a series of unique, natural and un-posed photographs. So you are free to focus on enjoying the now. Life moves on. But you can always look back and relive the moment" http://www.autographer.com/#home, April 23rd, 2014). Intimacy might be promoted in some ways as the actions required to use point-and-shoot cameras might draw attention away from the moment. However this does not solve the issue with intimacy identified above. In addition, it seems highly unlikely that lifelogs would replace other recording equipment as these have their own advantages - e.g. they might shoot photos with

higher quality, they have a display so one can check to see if the photo is as desired, it might be easier to aim a camera to create a specific angle, etc. - which means that the advantages identified by the makers of Autographer are only marginal. In sum, intimacy seems negatively affected rather than promoted by lifelogs. These above mentioned issues with intimacy are significantly reduced when lifelogs minimise the use of devices that capture audio or visual data about others.

There are other ways in which intimacy can be harmed unrelated to privacy. Real-time feedback from lifelogging device could be distracting. According to a Retrevo report approximately one in ten under-25 year olds checks their electronic messages during sexual activities (Eisner 2010). One may check the lifelog device, an action which would disturb one's immersion into the moment. In addition the feedback provided by the lifelog application could be the result of a skewed conception of sexual activity. This has been discussed in before (*5.2.1.1 Biases*), using the application 'Spreadsheets' as an example in which a rather masculine concept of sexual activity was promoted in which there seems little space for intimacy (and, indeed, more space for competitiveness). The lifelogger who conforms his activities to lifelog feedback would in this case fail to provide sufficient weight to intimacy. Conversely a well-designed lifelog application aiming for a high standard for information quality may improve behaviour by providing more balanced feedback while acknowledging the limitations of their device or they would refrain from providing feedback at all about elements that they cannot capture properly.

2) Respect for privacy protects one against embarrassment and humiliation. Failures to secure lifelog information against third party access and the sharing of personal information by lifeloggers could cause embarrassment and humiliation. The spread of data can be especially disconcerting because it can be distributed and accessed with such ease. People could be confronted with digital data at anytime, anywhere by anyone.[133] The issue of humiliation is exacerbated by the fact that lifelogs capture information automatically and lifelogging devices might not always visible or recognisable as such. Information that can embarrass or humiliate a person can even be captured accidentally such as the image of someone changing attire through an opening of the curtains.

---

[133] The fact that one can be contacted at any time is considered one of the more insidious characteristics of online bullying (Cotter & McGilloway 2011).

Sometimes government agencies cause the humiliation. As stated before, a right to privacy protects citizens by limiting the access of third parties such as governments to sensitive information. The extent to which government agencies respect privacy will affect the relationship between them and persons within their jurisdiction. An ordinary citizen stands in an asymmetrical power relationship towards government officials, which leaves citizens vulnerable to abuses of power of government officials that could humiliate or embarrass them. People might be vulnerable to having their data exposed to officials who repossess the device and access their data, something which has already been discussed in the chapter on privacy (*4.2.3.4 Concerns with enforced access*). However, these instances will only occur infrequently as officials will often not be in the position to demand access to a lifelog device.[134]

Lifelog technology may be used to capture and share personal information of an intimate nature aiming to embarrass or humiliate the other especially when wearable lifelog cameras are used. Indeed, one can imagine that partners living together may obtain intentionally or accidentally sensitive information from each other that can be used to embarrass the other. The antivirus company McAfee has published results which reveal that 13% of adults in the US have had intimate personal data shared by partners or friends (Eichorn 2013). An additional 10% have threatened to expose revealing photos online of former partners and almost 60% did. 'Revenge porn' is the public sharing of sexually explicit recordings without consent and with the aim to harm the subject.[135] Nonetheless the threat of

---

[134] The issues of embarrassment and humiliation related to governmental access to personal information are avoided when the subject is unaware of the fact that their information is being accessed. The unease caused by the access of personal information seems to be partly caused by the fact that the people feel that they have to display themselves. The access to personal data remains often unknown to those depicted on the images. Britain's surveillance agency UK Government Communications Headquarters (GCHQ) in conjunction with the US National Security Agency (NSA) stored millions of stills from webcam chats from Internet giant Yahoo under a surveillance programme named 'Optic Nerve'. Within six months in 2008 it stored communications of over 1.8 million Yahoo user accounts. Estimated is that the between 3% and 11% of the imagery collected by the GCHQ contained sexual explicit communications. Some of these pictures were accessed by the staff as the agency had reported difficulties filtering the explicit imagery. Despite the sensitive content these revelations seemed to embarrass the agencies involved and their governments more than the people whose data have been harvested as many (if not all) people are simply unaware that their data have been viewed. Similar to Yahoo webcam chats, one often will be often completely oblivious to the fact that someone has violated one's privacy by accessing or distributing lifelog information.

[135] There seems little legal and technological protection against the spread of such personal information. At least in the US, it is unlikely that the criminalisation of this phenomenon would be constitutional (Bennett 2013). Nevertheless, some states such as Florida and California seem to move towards a bill outlawing it (Clark-Flory 2013; Gershman 2013). There is anecdotal evidence that the sharing of this information can hurt the victims making it harder for them to engage in relationships again (Chiarini 2013; Filipovic 2013).

having information exposed does not deter people from sharing sexually loaded imagery as, for example 36% of Americans still intend to send romantic photos via text messages or other social media to their partners (Eichorn 2013) and 4% of the cell phone owning teenagers have sent sexually suggestive or nearly nude photos of themselves via text messaging primarily for romantic purposes (Lenhart 2009).

Sometime the threat of humiliation and embarrassment is used to blackmail the victim. The 15 year old Amanda Todd committed suicide after being extorted by a 30 year old man who had lured her into exposing her breasts (Wolf 2012). He threatened to show these images to her social network on Facebook if she would not comply with his demands for more imagery. She declined and he followed up on his threat by sharing the photos on Facebook, which resulted in her social isolation.

There is a related concern for those that capture sexual explicit activities of minors as that can be a felony. In the US a 20 year old man was found guilty for a child pornography offense when it appeared that he and his 16 year old girlfriend had made videos together with his cellular phone containing sexual explicit imagery (FBI 2012). Even though the activities captured were legal (both had reached the age-of-consent) and the data were not shared (he did not even transfer the videos from his phone) the mere act of videoing was illegal and this led to 18 months of federal prison time and a registration as a sex offender for the rest of his life.

It is yet unclear how the tendency to share personal information of intimate nature will progress as the ability to capture and spread personal information on this scale with this little effort is relatively novel and ways to educate and deal with this ability are still in its infancy. Deploying lifelog technology at home that captures imagery is expected to greatly exacerbate concerns as it would likely to result in more explicit images in the possession of others.

3) Sexual freedom can also be impaired because of a lack of privacy. A government that has access to information about citizens' intimate lives can more easily regulate this aspect of their lives. An illiberal or religious conservative government could use lifelogs to pursue those who have engaged in illegitimate sexual activity. In jurisdictions in which many forms of sexual activity, such as premarital or same-sex intercourse, are forbidden this could severely impair sexual freedom. In a similar vein, a government that respect privacy should not decry regulation that can only be enforced with unacceptable infringement of privacy.

The case of Griswold v. Connecticut (1965) illustrates this nicely. The US Supreme Court invalidated a law forbidding contraception as the execution of such a law would require violations of privacy.

Also one's social environment can restrict one's liberty. Social platforms such as social networking sites, forums, and even email or text messages services offer a terrific instrument to put someone in the pillory. Some platforms allow users to reveal the identity of the person depicted while the user identifying the person remains anonymous, e.g. anonymous forum post or fake Facebook/Twitter accounts. Recordings of a person entering a gay-club can raise questions even to those in communities that are considered quite tolerant. People struggling with their sexuality or otherwise facing taboos might be deterred from acting as they desire by the threat of being exposed. In more closeted communities mobs can be formed to hunt and attack people or in other ways ostracise those who are suspected of immoral behaviour.[136] In Russia, clips outing gay people are used to socially isolate them. Vkontakte' (VK) is the Russian counterpart of Facebook and used by some of it registered users as a platform to send threats to gay people, and share videos of rape and violence against gay people in order to humiliate and intimidate the Russian gay community (Parkinson 2014). The group 'Occupy Paedophilia', a group that does not distinguish between paedophilia and homosexuality, uses the website to come into contact with these men and arrange a meeting in which they assault them. They share these videos of these events so that the gay person recorded will face ostracisation.

Sometimes private surveillance by individuals might be extremely severe. As discussed in the chapter on privacy (*4.2.3.4 Concerns with enforced access*), some people might be forced by their environment to use lifelogs so that others can control their behaviour. One can imagine that in environments in which matters of sexual intimacy are mostly decided by the family and sexual freedom is limited, these abuses would be more likely to occur. Lifelogs would offer a great instrument to watch over these people and prevent them from committing social undesirable behaviour.

---

[136] In the Netherlands there is a Facebook page which offers the opportunity to report pillories that name and shame people from the Moroccan Dutch community so that action can be taken to prevent them (https://www.facebook.com/Meldpunt). Groen (2014) provides an anecdote about the distress that can be caused by sharing information. A video was posted online of a boy and a girl kissing, a clip which was captured by a CCTV camera from a Dutch government agency. As this behaviour was considered unacceptable in their community they got harassed and the girl attempted suicide as a result of the outcry in their community following it being shared.

Conclusion: Issues with bodily integrity will mostly be the result of lifelogs that are developed without sufficient safeguards for privacy. Lifelogs in which data are secured against third party access and which do not contain data that can be attributed to others would unlikely be instruments to harm bodily integrity. Other issues regarding bodily integrity are the result of content that contains biases.

Again, a careful design to avoid bias and promote privacy would mitigate many issues related to bodily integrity. In the situation that bias is avoid and privacy protected, lifelog technology may be useful to provide evidence to indicate misbehaviour or it may deter people from harming the other people's bodily integrity.

6.2.4 Senses, Imagination, and Thought

This capability consists of various elements and it seems appropriate to divide this capability into four elements.[137] This has been done because the elements differ quite substantially.

The first part states that one should be "able to use the senses, to imagine, think, and reason and to do these things in a "truly human" way, a way informed and cultivated by an adequate education, including, but by no means limited to, literacy and basic mathematical and scientific training" (Nussbaum 2003, 41).

Opportunities: Similar to the advantages for health, education might profit from an unprecedented amount of personal information and the ability to access it from a distance. Bell and Gemmell (2009) identified education as a domain of application, which can benefit from the usage of lifelogs. Lifelogs might be able to provide information to customise education by adjusting the curriculum and the form in which information is presented, e.g. to offer more time to students who are struggling while allowing faster learners to challenge themselves. Tele-education - in which the teacher teaches a student from a distance - might be supported with information about the behaviour of student. However the advantages to education in this regard are not as evident as for health in which the monitoring of body signals is evidently more vital. There are also some challenges that need to be overcome with this regard. The curriculum and the presentation of the curriculum could become increasingly determined by data and less by teachers, which could leave less space for other elements of teaching, such as care for the students, creating a safe and pleasant environment, and the identification of personal problems that a student might experience.

---

[137] The header might falsely suggest three elements.

Challenges: Lifelogs do not seem to interfere with education or a person's potential to become educated but Nussbaum aims for a wider concept including development and cultivation of the self. The "truly human" way which seems a terribly vague notion, might be thought to be compromised by the technocratic bias inherent to lifelogs (*5.2.1.1 Biases*). Because lifelogs are more accurate when retrieving information, the human ability to perceive and remember might be valued less and therefore will be less developed. A similar issue has been addressed before when lifelogs were said to cause cognitive laziness. However, there is no reason to believe that the consequence of using devices that are able to perform certain tasks more accurately will necessarily decrease one's senses and mental skills. Indeed as discussed above (*6.2.2 Bodily Health*), lifelogs might support memory. After all, lifelog information is too limited to be adopted uncritically and integrally. Indeed, the implementation of lifelog information requires human skill and reasoning, abilities which one has to develop.

The second part states that one should be "able to use imagination and thought in connection with experiencing and producing works and events of one's own choice, religious, literary, musical, and so forth" (Nussbaum 2003, 41).

Opportunities: There are also artists or people who will find inspiration in lifelogs or consider them a tool for art. The previously mentioned (*2.3.1 Brief history and current state of lifelogs*) Steve Mann uses his technology for art, for example by changing the content of his lifelog to alter the visual appearance of a scene (Mann 2003). Other examples of artists using lifelogs or lifelog-like devices are Stephen Cartwright who has been recording his latitude, longitude and elevation hourly since 1999 and Alan Kwan who captured 10 hours of video every day since November 2011.[138]

Challenges: There seems no obvious way in which one can fully quantify the elements that indicate the importance of religious, artistic or creative activities through lifelog devices or applications. There may be roundabout ways to capture indicators of the importance of these things such as capturing details that show the craftsmanship involved or the emotional reaction to the works. Computable aspects in the lifelogger's life could become more dominant such as living healthier, becoming more productive, and decreasing carbon footprint. These are the elements which the lifelogger can retrieve and for which he can most

---

[138] Information about the artists and their lifelog project could (at the 29th of April, 2014) be found at http://www.stephencartwright.com/ and http://www.kwanalan.com/#!lifelogging/ckt6.

directly see the results if he changes his behaviour based on lifelog information. The benefits of lifelogs for art or religion seem incidental while the failure of lifelogs to capture the importance of these elements can systematically undermine their place in society.

The third part states that one should be "able to use one's mind in ways protected by guarantees of freedom of expression with respect to both political and artistic speech, and freedom of religious exercise" (Nussbaum 2003, 41).

Opportunities: Lifelogs can allow an enormous amount of people to share information about their art or religion. As a result a huge increase in information about diversity and different perspectives is to be expected. Indeed, this could allow experiments of living in which people can use information to shape their lives differently to see what lifestyle suits them.

Challenges: Most of the concerns with this part of the capability stem from failures to protect privacy. The potential reductions of privacy facilitated by lifelogs can negatively affect freedom of expression and religion. In the case that information related to values and beliefs is accessible and distributed amongst citizens social or political pressure could arise that makes it difficult to voice dissent. Dissidents and/or insurgent populations can be tracked more actively and unrest could be identified at an earlier stage. Also the government might obtain information to incriminate or disrepute individuals or communities. The proposals of the US NSA to disrepute individuals that are radicalising others are an example of the latter (Greenwald, Gallagher & Grim 2013). These proposals were tested in a trial consisting of six individuals, all Muslims, who were identified as targets while none of them were accused of being part of terrorist plots. The NSA aimed to uncover personal information that could be used to undermine these individuals' reputation, authority and credibility through electronic surveillance. Following activists to disrepute them is not a novel practice in the US as J. Edgar Hoover's FBI already attempted this with Martin Luther King, Jr., whom Hoover considered a threat to the national security (Greenwald, Gallagher & Grim 2013). Sometimes the authorities might even proactively try to intimidate activists or dissidents based on data interceptions. Participants in the 2014 Ukraine protests got a text message from a government agency that translated to English read: "Dear subscriber, you are registered as a participant in a mass riot" (Walker & Grytsenko 2014). Currently the checks and balances in place to curb governmental power are insufficient to protect citizens against authorities and companies accessing and distributing data of consumers or citizens.

Lifelogs can hinder creativity or diversity. Even in places in which political and religious freedoms are protected by legal rights, failures to safeguard privacy could hinder the conditions necessary to develop or exercise a diverging political or religious view out of fear of expulsion. A photo of someone entering a church or visiting a mosque can raise questions about the person who may not be ready or willing to answer any of these. It becomes increasingly difficult to experiment when one has to account for these choices. After all, experiments with other lifestyles or religions might amount to nothing while the recordings of these experiments remain. Moreover, the benefits of religion or other lifestyles may be difficult to explain with lifelog technology or other recording technology because they often have no measurable advantage. A debate which is largely based on recorded data and tangible advantages may fail to properly account for these non-measurable aspects. Struggles with creativity or religion might be considered peripheral as their importance is non-measurable to those who do not experience them.

This lack of privacy is felt dearest in communities in which liberty is strongly curtailed. It is doubtful though that many people living in countries with oppressive regimes or within intolerant communities begin using lifelogs as the consequences of this information falling into the wrong hands can be severe.[139] Lifelogs for reasons of leisure will most likely be used in communities in which members can voice dissent and have diverging lifestyles without a blighting fear for prosecution or repudiation. However, this will not affect particular minorities that, unlike other groups, do have to fear this repression or are not allowed these liberties. As discussed before (*5.3.1.1 Diminishments by governmental agencies*) failures to respect privacy or reductions of privacy affect minorities the most (Reiman 1995). By reducing privacy, their freedom to decide matters for themselves might become (even more) compromised as information about their behaviour can be used to target it. More information about the behaviour of these groups can call stricter laws into being. Especially groups such as women, illegal immigrants, and new migrant groups who, in contrast to the rest of the populations, might experience less personal freedom and rights might be targeted.

The fourth and final part states that one should be "able to have pleasurable experiences and to avoid non-beneficial pain" (Nussbaum 2003, 41). The overall effect of

---

[139] Unless these technologies offer them clear advantages, e.g. Ai WeiWei's short-lived lifecasting project to protect him against the authorities and inform others about his situation. However this will not affect many people as discussed before (*5.3.2.1 Protection against authorities*).

lifelogs on this part of the capability seems ambiguous at least. One can both experience anxiety as well as joy from the use of lifelogs.

Opportunities: One may experience pleasure watching photos with sentimental value or one's own achievements. Bell and Gemmell (2009) mentioned the fact that lifelogs could leave precious recordings of loved ones who have passed away. Indeed, the possibility of establishing an archive with recordings of important events, such as one's wedding day, is used by the makers of Narrative Clip and the Autographer to promote their product. It seems to be a major reason for purchasing and using lifelog technologies.[140] This is somewhat puzzling as people currently possess so many recording devices that the use of lifelogs solely for this reason seems disproportional.

In addition lifelog technology may provide information about past experiences informing one about the things that one seemed to find most pleasant and the things that seemed unpleasant, e.g. the lifelog may be able to gather information about pain levels or stress levels. With this information the lifelogger may be able to avoid these situations. The obvious issue with this kind of information is that this information by itself can be unsettling. For example, what happens when the lifelog shows that one is most stressed in the vicinity of one's partner or children and how does it affect people's relationships?

Challenges: Lifelogs could decrease self-esteem by showing that one actually fails to achieve one's goals. For example, lifelogs might show that one's social life is actually poorer than expected or that despite one's best efforts one still fails to exercise sufficiently. One may also suffer distress when watching events that were unpleasant, such as the incidental capturing of an accident. Sometimes one may suffer distress and humiliation because information is spread in ways that one finds unsettling.

Lifelog feedback can cause anxiety to people not suffering from anxiety disorders as well. False positives or negatives can be a source of distress leaving it difficult for the lifelogger to pin-point the mistake, which is exacerbated when lifelog data are distributed to

---

[140] "The baby bump. The newborn asleep in your arms. The first toothy grin. The last days of nursery and the new school uniform. Autographer is made for life-logging the fleeting moments of parenthood. No fuss, no focussing: record how your little ones grow and change every day, with unique, natural, un-posed shots. Now you can capture every memory, even as life moves on." This is the text one can find on the Autographer website (http://www.autographer.com/#home, April, 23rd 2014). "The Narrative Clip ... Capture, store and relive special moments with the world's smallest wearable camera" is the text one can find on the website selling the Narrative Clip.

others making it difficult if not impossible at times to correct this information. Imagine lifelogs possibly falsely stating that one is more stressed in proximity to one's partner than being alone or with friends. Also the fact that lifelogs could present important but unverifiable information can negatively affect the lifelogger's emotional state. As discussed previously, the way one walks can increase one's susceptibility to assault (Gunns, Johnston & Hudson 2002). Knowing this information can provide a feeling of vulnerability. Another example would be a lifelog application that based on behavioural patterns can predict with great accuracy when someone intends to break-up, which is already possible using Facebook (Backstrom & Kleinberg 2014). These and similar more subtle findings could greatly disturb relations and cause anxiety while the lifelogger may have great difficulties establishing if the findings presented to them are correct.

Feedback can have implicit standards which are too demanding and/or unfair. In the scenario a situation was sketched in which the main person, Paula, was querying the lifelog to retrieve information about her spending time with her children (*2.5 Scenario*). If the lifelog only counts the times Paula is actively involved with the child, for example plays a game or reads a story, then cooking healthy meals or doing other things for them which do not require interaction, are disregarded. Spending sufficient time can become too burdensome causing anxiety and stress. A similar issue has been discussed in relations to the capability 'bodily health' and medicalisation. The recommendations to live a healthy life might become too burdensome. Indeed, the availability of so much detailed information about so many aspects of health such as sleep, exercise, and diet could encourage an unattainable want to achieve optimum results for all of them. This issue is exacerbated by the fact that lifelogs can capture information about many aspects relevant to the good such as the environment, health, education, *et cetera*. Living a good life can become very demanding. Meanwhile lifelogs will fail to capture all aspects relevant to the good making a life predominantly focusing on optimising results within the lifelog ultimately dissatisfactory. A related issue is that the descriptions provided by lifelog technology might project a specific understanding about events and people. As discussed before (*5.2.1.1 Biases*), lifelogs might infer information about the lifelogger such as gender, sexuality, or relationship status. These classifications might not fully capture the person described. Classifications that are ill-suited might confuse the individual, e.g. people struggling with sexuality might be confused by how lifelogs classify their sexuality or that of others, or cause anger because of the lack of recognition.

The causes for anguish can be minimised by carefully selecting and presenting information to ensure that information that may cause anxiety is avoided and that the lifelogger is aware of the limitations of the information presented to them. Because the issue can be addressed and there is an incentive to address this issue, as it may deter people from using lifelog technology, the issue is likely to be avoided.

Conclusion: There were four elements to this challenge. The effect of lifelogs on this capability is predominantly negative though minor. Overall, this capability is predicted to be slightly negatively affected mainly because of lifelogs' inability to capture non-measurable information and severely impaired when lifelogs will fail to protect privacy. Most issues regarding this capability are caused by a failure to safeguard the privacy of the lifelogger or others recorded by the lifelogger.

6.2.5 Emotions

"Being able to have attachments to things and people outside ourselves; to love those who love and care for us, to grieve at their absence; in general, to love, to grieve, to experience longing, gratitude, and justified anger. Not having one's emotional development blighted by fear and anxiety. (Supporting this capability means supporting forms of human association that can be shown to be crucial in their development.)" (Nussbaum 2003, 41).

Opportunities: Lifelogs can reveal information about the emotional state of the lifelogger or others. Lifelogs can inform the lifelogger about events that seem to be most enjoyable to the lifelogger or others by using facial, vocal or bodily signals to indicate activities such as laughing that can be used as indicators for pleasure. By offering information the lifelogger comes to know what events were most pleasurable or, conversely, which were least pleasant. When lifelogs show that a particular action causes distress to the lifelogger or someone else, the lifelogger informed by the lifelog can avoid situations in which the performance of these actions is necessary. The same goes for events that are pleasant. However, to obtain more information about the emotions of others would often require the use of visual or audio recordings which does not seem desirable for privacy. Moreover, wrongful or untimely inferences of emotions could cause distress. They could reveal that one either enjoyed or disliked things of which one would be unaware or that one was not ready to be confronted with.

Challenges: As mentioned in the literature review (*3.2.1.6 Impairing social interaction*), issues can arise because lifelogs reduce the need for physical human presence or even human interaction in obtaining and spreading information (O'Hara et al. 2006; O'Hara, Tuffield & Shadbolt 2009; O'Hara 2010). The availability of lifelog information means that information is communicated without the emotions that face-to-face encounters or other oral or written accounts can contain. If this would become the norm, society as a whole could develop characteristics similar to that of a person with autism or schizophrenia (Murata 2011). After all, lifelogs do not present information with subtle forms of empathy or compassion which would be the case with an oral or written history by most persons; emotions that can be lacking for people with autism. Baruch, to which Murata refers, coined the term 'autistic society' (2001). He identified domains in which the first signs of such a society became visible, such as online shopping, telecommuting, and e-mail. These media leave less space for affective emotional contact. Lifelogs further decrease the need for direct social contact, as, at least with e-mail, one obtains information written directly by another person. In addition, these media often fail to distinguish between trivial and nontrivial matters, a symptom that is also associated with people with autism. In the situation of lifelogs, they can store information about any event no matter how unimportant.

The result of being presented with information outside the context without human contact is that events could be judged more callously. The lifelog could *ex-post* present details about the event that were not known to the lifelogger. Therefore lifeloggers could assess events primarily on lifelog information so without considering the human emotions shaping the context in which these events took place and knowing details that may not have been noticed by the people involved. However, the fact that lifelogs may not directly present information with emotions so typically for people when communicating does not mean that there is no space for emotions when accessing lifelogs: lifelog will not be the sole sources of information – they have their shortcomings and some situations will not be lifelogged – and often lifelog information will not be used solely for a factual reiteration but as a means to reminiscence and invoke certain emotions – similarly people often consult photo albums for other reasons than to obtain a more accurate picture of the past. Indeed, more familiarity with lifelog information should make people increasingly aware that the lack of context is a distorting factor when assessing the event.

Lifelogs would also alter the importance of emotions in other ways. Lifelogs could make it increasingly unfavourable to show emotions. Lifelog devices could be able to capture

people's initial reaction or emotions more accurately than people would during face-to-face encounters. Emotions can become inescapable tell-tales about things one would prefer to hide.[141] Again this issue is largely dependent on the fact that lifelogs might gather information about others.

In addition, confrontations with information that one is not yet ready to be faced with can harm one's emotional development or one's emotional state. Untimely information may hamper development. Imagine again the person struggling with his relationship being informed about the lifelog's prediction of the durability of his relationship (as discussed in *6.2.4 Senses, Imagination, and Thought*). Developers should aim to avoid information that may upset the lifelogger or that may impede their privacy.

Conclusion: Overall, it seems that lifelogs have a marginally negative effect on this capability. Limiting information about others and minimising information that could upset the lifelogger are ways to tackle this issue.

6.2.6 Practical Reason

"Being able to form a conception of the good and to engage in critical reflection about the planning of one's life. (This entails protection for the liberty of conscience and religious observance)" (Nussbaum 20003, 41).

Opportunities: Lifelogs can aid self-reflection. With a lifelog one can obtain more information about the consequences of one's acts and the acts of others, which is particularly useful in a complex world where one has a lot of options to act in many different ways. However information is often scattered, unclear or unreliable making it difficult for people to autonomously develop a conception of the good and strive to achieve the goals associated with that. The lessening of resources and time required to obtain information allows people to set novel goals and to rearrange one's life, e.g. being able to reduce one's carbon footprint, live healthier, buy more fair-trade might become less demanding allowing persons to address these aspects while also having enough time and resources remaining to lead a fulfilling intellectual and artistic life. Reducing one's carbon footprint is a goal most people would endorse, but which might be daunting due to the multitude of ways in which one can affect the environment. A lifelog which could present the lifelogger with the effects of her behaviour without requiring much effort from her could be helpful. Besides increasing

---

[141] Facial expressions could reveal emotions (Yong Tao and Martinez 2014), as well as voice and speech (Scherer 2003).

understanding lifelogs could also be used to help the lifelogger to create the conditions that are most favourable to decision-making. Stress is an example of a condition that can impair one's ability to make decisions. By identifying situations that causes stress to the lifelogger the lifelog might aid the lifelogger to avoid these situations.

In order to do so, developers need to ensure that the content of lifelogs meets an acceptable standard of quality and is presented in a way that allows the average lifelogger to make use of this information. If lifelogs prove unreliable, incomprehensible or cumbersome to task, lifelogs will be unsuitable for critical self-reflection. It is by no means certain that lifelogs will offer this standard of information. Lifelogs might become popular even if they fail to provide a high standard of quality for information. The fact that lifelogs can contain information about moments that are considered milestones in the lifelogger's life might be sufficient for some to lifelog. The Narrative Clip and the Autographer seem mainly focused on the latter.

Challenges: There are also reasons why lifelogs might be unsuitable for developing a conception of the good. These mostly centre on the idea that lifelogs are by no means an ideal source of information and that they might reduce privacy. Most of these issues are stemming from concerns already identified in the chapter on autonomy. Potential biases have been discussed that can creep into the design of lifelogs thereby making lifelogs promote a value loaded concept of reality, which is quite limited when lifelog content is used integrally and uncritically (*5.2.1.1 Biases*). Moreover, a lack of privacy could demand conformity to existent values and beliefs (see *5.2.1.5 Creating a Panopticon* and *5.3.1 Challenges to executory autonomy*). Finally third parties such as corporations or governments are handed a powerful tool in the form of personal information to manipulate or otherwise control the lifelogger.

1) One cannot develop a conception of the good solely based on lifelog information because the 'overview' lifelogs provide is partial and selective.

The accuracy and vastness of lifelog information can coax lifeloggers to rely primarily on lifelog information rather than their 'own' observations and/or neglect aspects that fell outside the reach of lifelogs. Moreover, society could encourage the use of lifelogs rather than personal observations as lifelog information will often be more accurate in many ways than a human description. In such environments persons would judge events on lopsided information as lifelog information has its own limitations; for example, eating is

predominantly judged upon its effects on health and price rather than on non-measurable aspects such as its cultural or social importance. In the chapter on autonomy (*5.2.1.1 Biases*) several possible biases that can influence the design and content of lifelogs are mentioned.

Nonetheless, in many instances accurate empirical or other digital information can be useful for self-reflection. Moreover the fact that one can only conditionally use this source of information to form ideas about the good and the bad is an inherent characteristic of any source of information and therefore does not merit much weight. Furthermore, many sources of information that purposely aim to advance a particular view are, in fact, often accepted. There are many news outlets that promote a particular ideology sometimes even without explicitly stating so. In the situation that the lifelog company aims to promote a particular ideology it needs to inform the lifelogger.

2) Reductions of privacy might require the individual to conform to existing social, moral, and legal norms as was discussed in the chapter on autonomy. The fact that actions are increasingly visible requires a person to either remain unfazed by the gaze of others or to conform to the prevailing norms. Not everyone will have the strength to withstand social pressure. Indeed, the availability of this information could allow individuals, corporations, or governments to actually pursue people with different ideas. Corporations could financially punish people, exclude them from services and products, or diminish their opportunities for employment. Secret services and other government agencies have regulative, judiciary, and/or executive power and a wide-range of tools to their avail to track and persecute people based on personal information. Individuals can form mobs or threaten others with the risk of ostracism and social opprobrium. Benson (1991) describes the possibility that the enforcement of oppressive social norms may be so persuasive that the person experiencing them considers them a necessary and inevitable part of their reality rather than contingencies that can be avoided. As a result the person appropriates the norms as a given.

3) The fact that lifelogs offer so much detailed personal information allows third parties such as corporations to influence the behaviour and beliefs of the lifelogger. The content of lifelogs seems to be a marketer's Holy Grail. By using lifelogs a wealth of information is potentially available to assess the effect of advertisements on individuals. Information about how people react to messages can be made more readily available. Marketing campaigns can be adjusted so that they become most effective. Third parties may deduce from lifelog technology, which manipulation strategies are most effective.

Another strategy could be to influence the content of lifelogs, which is particular difficult to spot if the content cannot be verified by the lifelogger, such as stress levels, sleeping patterns, or other body signs. Another way of manipulating the lifelogger is to adjust content retrieval. Lifelogs require algorithms that determine the information that is provided when lifelogs are queried; a decision needs to be made what information is relevant and which is not. Often lifeloggers would have little insight into the workings of these algorithms and the interests they serve which would increase the power of third parties (Morozov 2013). Companies can adjust information retrieval to suit their purposes. Lifelogs can be used to promote any product or service, worldview, or ideology.

The possibility to use lifelogs as a vehicle for marketing is dependent on the access others have to data and their influence over the functioning of the devices and applications. In addition, the importance the lifelogger attaches to the information from this medium plays a role in the effectiveness of manipulation. If lifelogs are only sporadically consulted, then this issue would be minor.

Conclusion: Overall lifelogs seem to negatively affect 'practical reason'. Most of these issues are caused by a failure to secure the lifelog against third party interference and a failure to mitigate bias. Again, it seems important that lifeloggers is made aware of the limitations associated with lifelog content so that there is space for doubts and interpretation.

6.2.7 Affiliation

This capability is divided into two parts which will be discussed separately below. Both show that lifelogs will offer challenges rather than opportunities regarding this capability when they fail to safeguard privacy of the lifelogger and others. The first part reads as follows:

"Being able to live with and toward others, to recognize and show concern for other human beings, to engage in various forms of social interaction; to be able to imagine the situation of another. (Protecting this capability means protecting institutions that constitute and nourish such forms of affiliation, and also protecting the freedom of assembly and political speech.)" (Nussbaum 2003, 41-42)

Opportunities: There are reasons to believe that lifelogs can be beneficial to human relationships. Lifelogs can be used to show living and working conditions by capturing determinants of well-being such as nutrition, stress levels, housing, *et cetera*. This

information can be shared in order to create more understanding about the lifelogger's situation.

More empathy is created on the basis of videos and photos than by showing statistics.[142] According to Lahlou (2011) using recorder capturing visuals from the lifeloggers point of view, enables people to empathise with the person recording. Wearable cameras as used by lifelogs can create such visual information. Sometimes it even helps communication. For example, the use of a SenseCam can provide visual cues to children suffering from particular forms of autism to help them communicate and develop skills needed for independent living as well to provide more insight into their behaviour to parents and other carers (Hayes et al. 2010). However, lifelogs capturing images will most likely harm the privacy of others, which is likely to actually do more harm than good to affiliation.

Challenges: The idea of privacy as a necessary means for social relationships has been advanced by various scholars (Fried 1968; Rachels 1975).[143] Moreover the circulation of personal information could hinder a person to take part in social life.

According to Fried (1968) and Rachels (1975) people adjust their behaviour based on the kind of relations one has with a person. Rachels states that privacy is a necessary means to uphold a "variety of social relationships" (Rachels 1975, 326). In a particular role one behaves differently than in another; a warm and loving parent can be a cold negotiator professionally. This seemingly inconsistent behaviour can be appropriate and indeed necessary depending on the context in which it is displayed. Privacy provides the personal space needed to perform these roles. By behaving differently one does not *act* or behave hypocritically but one merely plays the part, which is most apt for the situation. Without privacy one cannot maintain these different personae (Rachels 1975, 330). The ability to gather and store information about others and make this information accessible could severely impair this ability as one would be unable to control one's personae. Even if, the behaviour displayed is acceptable and indeed common, one might still have a reasonable

---

[142] If the lifelogger would only be wearing a camera, which would be a limited lifelog, this would most likely also be the case. Information about the lifelogger would be gained by disseminating information about their environment rather than by watching him. By looking at footage taking from camera empathy is created. As in the movies, wearable cameras trick the viewer to take the perspective of the character by hiding him. These first perspective videos are in the movies called 'points of view shots' (also known as POV shots).

[143] The importance of friendship, although his concept of friendship differs from the contemporary one, was already mentioned by Aristotle who considered friendship necessary for human flourishing (Aristotle 1998, book VII and VIII).

interest to distance oneself from being associated with it in other contexts. Behaviour that is acceptable in one context could be inappropriate or unjust in other contexts. To refer to the previously given scenario (*2.5 Scenario*): the footage that portrays the manager as a drunkard is acceptable among friends but can undermine authority when viewed by others who may not distinguish between the different roles.

Fried (1968) has a somewhat similar argument. He considers privacy necessary "for the relationships of love, friendship and trust" (Fried 1968, 484). He specifies three manners in which privacy sustains or creates these relationships. First, privacy enables one to select the information, which, by itself, can be a way to establish and maintain relationships.[144] Secondly, persons vary the degrees of intimacy between people. A third party accessing or spreading this information could break the balance of intimacy achieved between individuals (Fried 1968, 485). Thirdly, some information is better not known to anyone else at all. Some ideas or thoughts are better kept a secret even if they are in fact common and benevolent. Another issue, and this point differs from the ones made by Fried and Rachels, is that remembering is also part of being friends; one remembers what one's friends reveal because one has an interest in them. Capturing information would diminish the need to do something that is part of being friends, namely remembering. By doing so lifelog technology promotes vices that undermine friendship. Finally lifelogs could potentially reveal things that can hurt relationships. Lifelog applications could offer information such as predictions of the likelihood of a partner wanting to end the relationship based on information obtained from emails or social networking sites. This could cause anxiety especially as the choice between trusting the application or the person is a leap of faith. The actual feelings of the other are non-measurable while the algorithms are likely to be too complex (if available at all) to be scrutinised by the lifelogger.

The second part of the capability of affiliation reads as follows: "Having the social bases of self-respect and non-humiliation; being able to be treated as a dignified being whose worth is equal to that of others. This entails provisions of non-discrimination on the basis of race, sex, sexual orientation, ethnicity, caste, religion, national origin" (Nussbaum 2003, 42).

Opportunities: There are some advantages expected from lifelog technology. Lifelog technology could capture the behaviour of bullies, racists, or people otherwise attempting to

---

[144] Rachels (1975) advances a similar argument. Because people can choose to reveal themselves to others, the sharing of information is by itself a sign of intimacy and trust. People bond through sharing information.

harm people. Another advantage is that lifelog technology may show similarities between people. By doing so, lifelog technology may show that there is no basis for discrimination implicitly assuming that existing discrimination is the result of rational yet ignorant people who would stop being racist when their claims are refuted. However there is currently already a wealth of information available that disproves most racist claims. Finally, the wide variety of lifestyles made more visible through lifelogs may inform people about diversity and force them to accept it as a given. These advantages would often require the capturing and sharing of personal information about others, which is accompanied with far greater concerns for privacy and autonomy as discussed in previous chapters. In addition, at present, information about cultural diversity is readily available. In summary, these advantages for non-discrimination seem minor or require capturing information about others.

Challenges: Lifelogs could facilitate discrimination. The digital accessing of personal information can take place without the direct involvement or awareness of the person being searched or without sufficient checks and balances in place to prevent discrimination. These searches could be based on prejudice or undertaken for discriminatory purposes. For example, government officials and private individuals may use lifelogs to discredit specific individuals based on their religious beliefs by searching and revealing information that might not be illegal but can disrepute them, which seemed to be a method explored by the UK GCHQ with Muslim conservatives (Greenwald, Gallagher & Grim 2013). As a result existing prejudice can flourish as particular minorities who, as a result, can be searched more often and have their privacy more often violated without citizens being aware of this fact.

When discussing the capability 'practical reason' issues with algorithms were discussed (*6.2.6 Practical Reason*). Algorithms can be so complex that it can be impossible to distinguish the weight of a particular variable on individual results. An issue with regard to discrimination is that variables that are discriminatory can be concealed by algorithms that are impossible to check. As a result discriminatory variable become part of governmental or corporate decision-making while citizens or consumers have little ability to prevent this from occurring.

Conclusion: Once more, this capability seems to largely depend on developing lifelogs in a way that they conform to privacy requirements. If lifelogs are developed so as to avoid capturing information about others, secure them against third parties accessing their data and limit the purposes to which the data are used, then this capability seems unlikely to

be significantly harmed. In contrast, when there are insufficient protections for privacy and security, then lifelogs are harmful with regard to this capability.

6.2.8 Other Species

"Being able to live with concern for and in relation to animals, plants, and the world of nature" (Nussbaum 2003, 42).

Opportunities: There are reasons to believe that lifelogs might prove useful to the environment in a similar way as they are beneficial to health. As the effect of lifelog technology for the environment is quite similar to its effect on health, this capability will be discussed more briefly. The effect of lifelog technology on the behaviour of the lifelogger will be discussed first and the effect on the environment of the lifelogger is discussed second.

1) Lifelogs can be a tool for people to become more efficient and waste less, which would mean a benefit to the environment. For instance, lifelogs could be used to reduce the usage of fossil fuels. Diminishing energy usage has numerous advantages such as preventing: "human health problems caused by air pollution from the burning of coal and oil; damage to land from coal mining and to miners from black lung disease; environmental degradation caused by global warming, acid rain, and water pollution; and national security costs, such as protecting foreign sources of oil" (UCS 2002). Globally, households emit 72% of the greenhouse gasses of which 20% is for food, 19% for housing and 17% for mobility (Hertwich & Peters 2009). Much of one's current carbon footprint is determined by dietary intake, mobility, the products and services purchased, and housing. These are choices that are related to lifestyle and, as a result, people can reduce their carbon footprint by adjusting their way of life. There seems no reason that lifelogs could not provide complex information relevant to the preservation of the environment and present this in a way that is understandable to lay-people. Life cycle assessments (LCAs) showing the environmental impact of individual products present information that would be time-consuming for a consumer to track but potentially valuable in reducing consumption that is harmful (Rebitzer et al. 2004). Also the fact that one's achievements are tracked might be motivating, especially when lifelogs facilitate the sharing of information or the setting of long-term and short-term goals. Feedback on energy consumption might be a tool to save energy (Fischer 2008). Similar assessments for food (nutrition greatly affects one's carbon footprint), can be used helping people maintain diets that are environmentally sustainable (Weber & Matthews 2008). There are many other pressing issues regarding the environment that can be alleviated.

For example, issues caused by urbanisation such as congestion may be addressed through lifelog technology by showing the routes and times that cost the least resources and time to commute alleviating the local infrastructure. The benefits to the environment are not intrinsic to lifelog technology, but the lifelog technology needs to be developed in a way that the lifelogger can retrieve information about LCAs or other indicators of their carbon footprint.

Finally, although this advantage might prove ever so small, lifelogs might facilitate a paperless existence avoiding costs to the environment associated with the storing and production of paper. Becoming paperless has been a motivation behind lifelogging technology since its origins as it was part of the MyLifeBits project. Gordon Bell claims to have lived paperless for more than a decade (Greenemeier 2014; Microsoft 2014).

2) The information lifelogs provide could also create an environment in which concern for the environment is stimulated. Similar to bodily health, the fact that more information can be gained about people's influence on the environment might create more responsibility and pressure on them to prevent harm to the environment. Indeed, in case governmental agencies and authorities are allowed to access data about behaviour affecting the environment, governments could use this data for policy and legislation. In order to do so, data could be anonymised and participation subject to an opt-in procedure so as to protect the privacy of the lifeloggers. Also the effect of the lifelogger behaving more environmentally friendly is likely to affect others, e.g. changes in diet are likely to affect those close to one as well. Moreover lifeloggers will likely share their experiences and knowledge creating communities and responsibilities for others to improve their behaviour.

Challenges: Lifelogs can pose two small challenges to the environment.

1) The use of lifelogs might become a burden to nature. The storage of data and applications costs energy and other resources and the fabrication and disposal of lifelogging devices might harm the environment. First of all, the storage of data costs energy. Of the total electricity approximately between 1.7% and 2.2% in the US, 2.2% and 3.3% in the UK, and 1.1% and 1.5% globally was utilised for data centres and this amount is slowly increasing (Koomey 2011: SCDI 2010). However, there is reason to believe that this issue is already being dealt with. Koomey (2011) states that the rapid growth in energy usage experienced between 2000 and 2005 slowed down between 2005 and 2010. Considering the vast amounts of data already stored and the fact that servers at most consume between 2.2% and 3.3% of the total energy it seems that lifelogs will not make much of a difference in the total usage of

energy. Moreover, data servers seem to become more efficient while devices are using less energy (Clancy 2013; Koomey 2011). In addition there is an incentive to minimise the energy consumption of wearable device and applications as extended battery life would allow the devices to function autonomously for longer while it would be cheaper and more convenient for consumers to operate these devices. The fact that both consumers as well as corporations have an incentive to minimise expenditure on energy, energy usage does not seem to be a pivotal issue.

2) Lifelogging devices can be made using materials and production methods that might harm the environment or the workers involved in the production, which was the case with smartphones (Bradsher 2010; Greene 2012). However, the fact that lifelogging functionality can be integrated into devices that are already used in daily life, such as smartphones, reduces the weight of this concern considerably. There would be no additional costs attached to lifelog devices. Moreover, there are signs that 'conflict minerals' are becoming an issue for companies and legislators with US legislation coming into effect that requires companies to publicly disclose when they use conflict minerals (Dodd–Frank Wall Street Reform and Consumer Protection Act 2010), technology giants such as Microsoft, Apple and Intel, Philips and AMD taking measures to improve the sourcing of minerals (Lezhnev & Hellmuth 2012) and the EU that has been planning similar legislations (European Commission. 2014). The fact that these issues are firmly on the political agenda makes it probable that they will be accounted for.

Conclusion: Overall lifelogs seem beneficial to the environment. Although there are some challenges, these are small and outweighed by the advantages. However, these advantages can only be realised when lifelogs are designed to provide information relevant to protect the environment.

6.2.9 Play

"Being able to laugh, to play, to enjoy recreational activities" (Nussbaum 2003, 42).

Opportunities: There are advantages to be expected from using lifelog technology. Autographer advertises on their website (http://www.autographer.com/) that by using their device one can enjoy activities without having to take photos. Also the content itself can be enjoyable. The lifelogger could enjoy revisiting events with the lifelog technology. The functionalities of lifelogs can be pleasant as well. A lifelog that can keep track of personal

belongings can be convenient: the ability to search a lifelog to find where one last left one's keys is less of a stressful event than turning one's room upside down. Another opportunity lies in the entertainment sector. The wealth of personal information could allow customisation of entertainment such as games, social interactions, television, radio, and films. Moreover, lifelogs may empower devices with data that are designed to convenience the lifelogger such as ambient intelligent devices. Lifelog data would be transferred to these devices that would use these data to adjust their functioning to suit the preference of the lifelogger. However, to achieve this, the devices and services need to be made compatible with lifelog technology. In addition the lifelog could be used to set goals to spend more time on leisure. Lifelogs could also inform one about the time made available by the lifelogger for leisure. Lifelog technology seems to offer great potential for the capability play.

Challenges: Lifelogs can have negative effects on one's state of mind, which may negatively affect one's ability to play. There have been several negative consequences of using lifelog technology discussed that can negatively affect one's mental state. Such issues have been discussed before when dealing with the capabilities 'emotions', 'affiliation', 'bodily integrity', and 'senses, imagination, and thought', e.g. causing embarrassment and humiliation that make one unable to enjoy activities. Other negative effects on one's ability to 'play' could occur as lifelogs could draw attention away from the importance of recreational activities by focussing too much on other aspects, such as health. However, current lifelog devices such as the Narrative Clip and the Autographer seem mostly directed towards capturing recreational activities and other enjoyable activities. The latter effect seems negligible. In addition, it seems unlikely that people would want to use a technology that mostly frustrates them making this issue less likely to occur.

Conclusion: Lifelog technology seems to have the potential to benefit this aspect of the good. Some concerns with 'play' are related to a failure to address challenges related to the quality of information and privacy.

6.2.10 Control over one's Environment

Also this capability consists of various parts that will be addressed separately. The effect of lifelogs seems ambiguous.

The first part states that one should be "able to participate effectively in political choices that govern one's life; having the right of political participation, protections of free speech and association" (Nussbaum 2003, 42).

Opportunities: Sousveillance and/or sharing information about living conditions can spark change or offer protection against overzealous or dictatorial governments or other parties negatively influencing freedom. Examples are the Arab Spring in 2010 in which photos and videos of abuses by governmental officials led to further public outcry. Moreover lifelogging might show the innocence of the lifelogger and protects the lifelogger by informing others about their goings-on. Hasan Elahi and Ai WeiWei used technology to show that they were harmless and, in the case of WeiWei, also that he was safe.

However, as Morozov (2011) remarked, digital information by itself is insufficient to protect citizens against government agencies and often only undermines the position of citizens vis-à-vis governmental agencies. According to him, recordings about poor working conditions or abuses by officials are insufficiently to organise and mobilise the people and/or the authorities in question can fail to react on this information. He seems right. After all, sometimes abuse is supported and encouraged by dominant communities within society, which is arguably the case in Russia in which the LBGT community suffers from abuse (Human Rights Watch 2013). Indeed, in Russia the capturing and sharing of personal information through digital means seems to worsen the situation by further spreading fear and repression. Currently Vladimir Putin is accused of using widespread conservative sentiments against the LBGT community to better his position by introducing laws forbidding gay 'propaganda' amongst children (Aron 2013; Rose 2013). The economic slump experienced in Russia was said to be hurting his support and populist measures were needed. In addition, ordinary citizens are unlikely to be able to interfere when another ordinary citizen on the other end of the world disappears, stops lifelogging, or shares their bad experiences, leaving them powerless when injustice has been revealed. Moreover, according to Morozov, governments can profit more from technology than the users would as the authorities can influence the development of technology and have more tools to gather data and signal early forms of unrest (Morozov 2011). His claim is substantiated by the recent revelations about the NSA weakening encryption.[145]

---

[145]Citizens are not completely powerless. Measures taken by companies such as Google providing better encryption (Google 2014) as a reaction to the popular outcry and the loss of consumer trust is an indication that

Challenges: Three challenges with political participation have been identified. The first is using lifelog data to create a technocracy in which people have less of a say. The second is that digital processing of personal information can obscure transparency necessary to control the behaviour of government agencies and/or corporations. The third is that a lack of privacy can hurt political freedom.

1) There is another way in which lifelogs could affect political participation negatively. Lifelogs can facilitate the creation of a technocracy. Maybe even without violating privacy, the access of the authorities to lifelog data could harm political participation. Lifelog providers in theory could offer data to government agencies anonymously and in bulk leaving no possibility to attribute data to specific individuals. In The Netherlands the Dutch police purchased collective anonymous data about speeding from the navigator company TomTom to better their policy (NOS 2011). Government agencies could use these data to design policies. As a result these policies are primarily based on data rather than on the political participation of citizens. After all, data can often provide accurate factual information that seems less ambiguous than the opinions of people which is quite clearly the case in the previous example. However data are not necessarily suitable for policy. As discussed before, sometimes data may contain bias (*5.2.1.1 Biases*). Furthermore data may fail to adequately reflect the values and beliefs of the citizens as behaviour does not always reflect how people want to act or ought to act.

2) As discussed before (*5.3.1.2 Diminishments by corporations*), individuals could increasingly become reliant on algorithms to determine one's entitlements. These algorithms could be complex or hidden making it impossible for lay-people and sometimes even the experts to tell the weight of certain variables. Google's algorithm for search, their core business, is so complex that even experts working in Google cannot fully explain individual results (Pariser 2011). The complexity and opaqueness of the algorithms makes it difficult for laypersons to criticise their output. For some areas the use of algorithms to make important decisions seem inappropriate as one would want citizens to support or criticise the outcomes. Citizens may have difficulties criticising the policies and actions of government agencies that are the result of the processing of data. A critical assessment by ordinary citizens can be

---

consumers exert a firm influence on the development of the technology which does not annul the power of the authorities but at least provides a counterweight against it In addition one could consider the announced reforms of security agencies and data storage policies by US president Obama as an improvement (Ackerman 2014) but it is doubtful if these reforms are significant or indeed improve the situation.

difficult because citizens could lack access to the data used and have little information about the algorithms, which could be complex. The government agencies that use these data should be able to explain which information they use and the weight they give to this piece of information for ordinary citizens to check their outcomes but may fail to do so and just refer to procedures in place.

3) The lack of privacy caused by lifelogs either capturing information about others or by lifelogs being accessed by third parties could impair the lifelogger's ability to participate freely in the political debate. The fact that third parties, such as members of one's social environment, companies, or governments, could access personal information can limit the freedom people enjoy regarding political choices. As became clear when discussing the capability 'senses, imagination, and thought' governments could choose to target political activists in order to disrepute them. These issues are solved by protecting lifelogs against third party access.

The second part states that one should be "able to hold property (both land and movable goods), and having property rights on an equal basis with others; having the right to seek employment on an equal basis with others; having the freedom from unwarranted search and seizure. In work, being able to work as a human being, exercising practical reason and entering into meaningful relationships of mutual recognition with other workers" (Nussbaum 2003).

Opportunity: First, lifelogs are an industry, which is an effect quite independent on the functioning of the lifelog. Moreover, lifelogs could improve working conditions. Finally, they are useful in preventing or addressing crimes.

1) A liberal argument to allow lifelogs is that there is a whole industry behind their development and production. By rendering lifelogs ethically undesirable and call for the abolishment of their development, one propagates the closing down of an entire industry including the development and commercialisation of lifelogs. The ample devices and applications that have been developed or are currently being developed show a commercial interest in lifelogs. To illustrate this point, Memoto, the company behind the Narrative Clip, gained their starting capital through crowdsourcing and reached over 1100% of their target sum of $50,000 (Oskar K 2012). Also the usage of lifelogs can be profitable for the lifelogger as he can save money by becoming more efficient (e.g. he can use the lifelog to shorten his commute or save on his energy bills) or he can even sell his data provided this is appropriate.

Moreover lifeloggers can use their lifelogs to improve their professional skills (which has been discussed in the chapter on becoming a lifelogger (*7.2.3.3 Positional goods*). The ability to capture and retrieve conversations and actions can be beneficial for some jobs.

2) Lifelogs might be used to improve the working conditions of the lifelogger or those of others, e.g. shared information about working conditions can be used to force companies to change their policies for the better. The working conditions within one company can be used as an example for other companies by comparing lifelog information from lifeloggers. Moreover lifelogs might be used to provide more insight into the production of particular products and services. Similarly to how lifelogs might offer more information beneficial to health, lifelogs might be made to show if the products and services purchased are offered under fair trading conditions. In retrospection the lifelogger can see if the products bought are actually fair-trade and if he should return his purchase or keep purchasing these products.

3) Lifelogs can also be used to protect property by preventing crimes. One such an offence is identity fraud. Identity fraud can only be committed when one has the information needed to pretend to be someone else.[146] A lifelog can provide of the identifiers. Nonetheless, in case of lifelogs, they can both facilitate and combat fraud. In 2012, there were roughly 12.6 million victims of identity fraud in the US alone (Javelin Strategy & Research 2013). Identity fraud can only be committed because of insufficient identification techniques or human errors. Information offered by lifelogs could be used to improve procedures to establish one identity or to offer information to expose the fraudulent practices. Credit Card Company MasterCard is currently running an experiment in which they check the location of the credit card holder with a smartphone when a purchase is made (Gibbs 2014). If the smartphone and the purchase appear at different locations at times of the purchase then that might be a sign that the credit card is used by someone else. With identity fraud the burden of proof lies with the victim as the person whose identity was stolen has to prove that it was not her. Lifelogs make this information available without much ado. The longevity of lifelog information can be particularly beneficial as identity fraud is sometimes only exposed after a while.[147] It is important to bear in mind that there are many technologies and activities that leave a digital trail that can be used for identity fraud. In case lifelogs can be secured against third party access, the ability of lifelogs to provide the lifelogger with an 'alibi' is not as common for other technology and might be very useful.

---

[146] "Identity fraud is fraud committed with identity as a target or principal tool" (Koops & Leenes 2006, 555).
[147] People can be unaware of the contracts being arranged outside their knowledge on their name.

Lifelogs can also protect people against corruption. In some countries it is important to disprove claims of other people, who can falsely accuse others in order to claim financial compensation. This explains the reason why many drivers of motor vehicles use dash cams: drivers in Russia and other parts of the world use dash cams to obtain legal evidence to protect them from getting swindlers staging road accidents (George 2013). In countries where corruption is rampant, the possibility to provide evidence is a valuable asset to avoid false claims. However, in other countries or in other contexts in which one does not have to fear the consequences of corruption these recordings of other people are disproportional.

Challenges: However, there may also be a negative consequence for property and employment. The story of Ashley Payne (*5.3.1.2 Diminishments by corporations*), who lost her job as a teacher, showed that people may lack understanding over how information is spread and/or interpreted and the consequences of that. Data brokers might obtain access to lifelog data and could use them to determine one's financial position and eligibility for certain financial services or suitability for certain jobs. One may be unaware of the existence of these profiles or unable to correct them. Moreover, companies might search for personal information on the Internet about future employees to determine their suitability. Again this is a challenge arising from a failure of lifelogs to protect privacy, or in the case of Payne, from a failure to protect one's own privacy.

Conclusion: Based on the first part of this capability, lifelogs will have a predominantly negative effect provided that lifelogs cannot be secured against government agencies attempting to gain access. However, judged on the second part of this capability lifelogs seem to primarily offer benefits. The issues associated with this capability are, again, largely dependent on securing the lifelog against third party access. Protecting privacy will avoid most of the challenges identified above.

6.2.11 Summary

It is remarkable that most capabilities can in some way be promoted or hindered by lifelogs. The good is formulated after the CA developed by Nussbaum (2003). The capabilities 'bodily health', 'other species', 'play' are expected to be positively affected. 'Life', 'bodily integrity', 'senses, imagination, and thought', 'emotions', 'practical reason', affiliation', and 'control over one's environment' are expected to be negatively affected. Most of the issues with the good in relation to lifelogs are caused by a failure to protect privacy or autonomy. Indeed, in case privacy is protected most harm against 'life', 'senses, imagination, and

thought', 'practical reason', 'affiliation', and 'control over one's environment' and 'bodily integrity' is avoided. Again, a checklist is provided in the appendix to identify issues swiftly (*Appendix C: Checklist for beneficence*).

Nonetheless there is much difference to the degree to which lifelogs affect some capabilities. The aforementioned 'life' seems relatively unaffected while bodily health and the environment can be greatly promoted. Also there seems much difference between the effects they have; for 'bodily health' lifelogs seem to have a predominant positive effect while for 'affiliation' the effects seems primarily negative.

Another comment to be made is that the promotion or hindrance of capabilities are partly determined by the design of lifelogs and if they are designed as to respect other principles, such as respect for privacy and autonomy. 'Bodily integrity', 'senses, imagination, and thought', 'emotions', 'practical reason', 'affiliation', and 'control over one's environment' are at least influenced by the ability of designing lifelogs to respect privacy. 'Bodily health', 'bodily integrity', 'senses, imagination, and thought', and 'practical reason' are dependent on the ability of lifelogs to respect the autonomy of the lifelogger and others.

Finally, due to the possibility of variation in design for lifelogs it is unclear which capabilities will be promoted or hindered. Many of the challenges as well as many of the opportunities identified in this chapter depend on the design of lifelogs, rather than them being intrinsic to lifelogs. There are four potential outcomes when weighing the good promoted by lifelogs:

1. The technology will principally promote the good.
2. The technology produces neither the bad nor the good.
3. The technology will principally promote the bad.
4. The outcome is unclear.

Because there is still much uncertainty at this stage about the design of lifelogs and lifelogs can both promote as well as harm the good, the result of this discussion is that the outcome is yet unclear. The reason is that lifelogs have both the potential to do good as to harm depending on their design.

If one would consider the few devices explicitly designed for lifelogging currently available, namely the Narrative Clip and the Autographer, exemplars for the current state of lifelog devices, the technology will principally promote the bad as they offer too few benefits

for lifeloggers or others affected. Their developers or marketers seem mostly concerned with offering convenient ways to capture trivialities. Currently the technological expertise may be missing to realise the opportunities advanced future lifelog technology could. Realising the opportunities can be technological difficult. Many of the benefits require expert knowledge which could make the device too expensive to be attractive to be developed or purchased. Assessing the further development as ethically desirable is a leap of faith: one has to trust that the further development spurs innovations that will lead to a future generation of devices realise their opportunities and, in balance, will promote the good. Some expansion of functionality is made more likely as the limited use of lifelogs could impair the adoption of the technology. In this stage in which lifelogging device may not offer much additional value they might not reach a major target market. For lifelogging devices to increase their market share they need to improve their functionality. Hopefully this functionality will not solely mean creating more information about increasing convenience (by allowing the lifelogger to find their keys or capture special moments with even less effort) but means actually improving capabilities.

6.3   Recommendations

To provide recommendations for beneficence is complex as there are many (diverging) capabilities. First of all, privacy and autonomy play a part in this as control over data and the quality of data are factors that influence the benefits and harms expected from lifelogs. More importantly, different capabilities such as 'bodily health' and 'environment' require the lifelog to deliver a high standard of information and expert knowledge. However, there are some general recommendations that can function as a heuristic tool to create the greatest possible balance of good over harm.

1. Identify possible challenges: Developers should assess the potential challenges to beneficence. This is the most general and the most evident recommendation but nonetheless important. Developers building lifelogs should assess how their technology could harm the lifelogger or others recorded by the lifelogger and develop ways to avoid this harm from happening. A 'value sensitive design'-approach or the help and knowledge of disciplines outside engineering and computing science can be beneficial, such as psychology, medicine, ethics, and environmental studies.

2. Identify possible opportunities: Developers should assess the potential opportunities for beneficence. Information can be useful in several ways but information has to be

240

presented in a way and form that is constructive to realise the opportunities. The opportunities are likely to be realised only with a conscious effort to achieve them, as the benefits from lifelogs are by no means self-evident.

3. <u>Involve experts:</u> Lifelog developers should involve experts capable of identifying issues and benefits and able to guide the development of the technology so that the benefits are reaped and the issues solved. Realising the opportunities is not self-evident and often requires expert knowledge. A multidisciplinary approach in which knowledge from various disciplines necessary for an ethical development of lifelog technology, such as communication studies, psychology, ethics, and medicine. If the lifelog aims to promote a capacity the information as well as the presentation should suit the purposes of this capability.

4. <u>Address concerns regarding privacy:</u> The previously provided recommendations to safeguard privacy should be followed (*4.6 Recommendations*). Harm is often resulting from failures to protect privacy of lifeloggers and non-lifeloggers. Safeguarding privacy by following the provided recommendations will alleviate some of the concerns regarding beneficence, such as for the capability 'bodily integrity'.

5. <u>Address concerns regarding autonomy:</u> Also, the recommendations to safeguard autonomy should be followed, e.g. a high standard for the quality of information can benefit lifeloggers and non-lifeloggers. In the following as well as in the previous chapter, recommendations are offered that can be helpful to address concerns for the autonomy of lifeloggers and non-lifeloggers (*5.4 Recommendations* and *7.3 Recommendations*).

6.4 Conclusion

Beneficence has been discussed as a principle of proportionality following Frankena, in which one should promote the greatest possible balance of good over evil (Frankena 1973). To define what is good and evil a list of capabilities is advanced. For lifelogs to harm or benefit means that they would either hinder or promote any of these capabilities.

A discussion about each separate capability showed that lifelogs have the potential to affect most of them. However, the effect on a particular capability could both be positive as well as negative. Both the positive as well as the negative effects were usually dependent on the design of the lifelog. By designing the lifelog carefully one could develop lifelogs in a

way they would mostly promote the good and do little harm. Often the negative consequences were caused by failures to either respect privacy or autonomy. By solving issues with these principles, one would minimise most harm. Moreover, the effect could be strong or weak depending on the capability. Some capabilities remained nearly unaffected while others could be greatly affected.

Finally, five recommendations are presented to alleviate concerns with beneficence. Again, because some capabilities depend on the ability of lifelogs to promote autonomy and privacy or leave them unaffected, these recommendations should be complemented by the recommendations made regarding privacy and autonomy.

Bibliography

Ackerman, S. 2014. Obama formally proposes end to NSA's bulk collection of telephone data [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/2014/mar/27/obama-proposes-end-nsa-bulk-data-collection [Accessed 31-03-2014].

Allen, A.L. 2008. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74.

Aristotle. 1998. *The Nicomachean ethics,* translated by Ross, W.D. Oxford: Oxford University Press.

Aron, L. 2013. *Sowing the Dragon's Teeth: The Kremlin's Reactionary Policies*. Washington: American Enterprise Institute.

Backstrom, L. & Kleinberg, J. 2014. Romantic Partnerships and the Dispersion of Social Ties: A Network Analysis of Relationship Status on Facebook. *Proc. 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)* [Online]. Available from: http://arxiv.org/abs/1310.6753 [Accessed 02-04-2014].

Bailey, J. & Kerr, I.R. 2007. Seizing Control? The Experience Capture Experiments of Ringley & Mann. *Ethics and Information Technology*, 9(2), pp. 129-139.

Baruch, Y. 2001. The autistic society. *Information & Management*, 38(2001), pp. 129-136.

Beauchamp, T.L. 2013. The Principle of Beneficence in Applied Ethics [Online]. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Winter 2013 Ed. Available from: http://plato.stanford.edu/entries/principle-beneficence [Accessed 08-12-2013].

Beauchamp, T.L. & Childress, J.F. 2009. *Principles of Biomedical Ethics: Sixth Edition*. New York & Oxford: Oxford University Press.

Bell, G & Gemmell, J. 2009. *Total Recall: How The E-Memory Revolution Will Change Anything*. New York: Dutton.

Bennet, M. 2013. *Are Statutes Criminalizing Revenge Porn Constitutional?* [Online]. Available from: http://blog.bennettandbennett.com/2013/10/are-statutes-criminalizing-revenge-porn-constitutional.html [Accessed 10-12-2013].

Benson, P. 1991. Autonomy and Oppressive Socialization. *Social Theory and Practice*, 17(3), pp. 385–408.

Bernstein, M.S., Bakshy, E., Burke, M. & Karrer, B. 2013. Quantifying the Invisible Audience in Social Networks. *CHI 2013, April 27–May 2, 2013*.

Bradsher, K. 2010. Challenging China in Rare Earth Mining [Online]. *The New York Times.* Available from: http://www.nytimes.com/2010/04/22/business/energy-environment/22rare.html?pagewanted=all [Accessed 16-12-2013].

Brin, D. 1998. *The Transparent Society: Will Technology Force Us to Choose Between Power and Freedom?* Reading: Perseus Books.

Brotsky, S.R. & Giles, D. 2007. Inside the "Pro-ana" Community: A Covert Online Participant Observation. *Eating Disorders: The Journal of Treatment & Prevention*, 15(2), pp. 93-109.

Carr, N.G. 2010. *The Shallows: What the Internet Is Doing to Our Brain.* New York, London: W.W. Norton & Company.

Chen, Y. & Jones, G.J.F. 2012. What do people want from their lifelogs? *IN: 6th Irish Human Computer Interaction Conference*.

Chiarini, A. 2013. I was a victim of revenge porn. I don't want anyone else to face this [Online]. *The Guardian*. Available from: http://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change [Accessed 10-12-2013].

Christensen, S.S. & Williams, J.L. 2011. Orange County Man Who Admitted Hacking Into Personal Computers Sentenced to Six Years in Federal Prison for 'Sextortion' of Women and Teenage Girls [Online]. *FBI Los Angeles Division*. Available from: http://www.fbi.gov/losangeles/press-releases/2011/orange-county-man-who-admitted-hacking-into-personal-computers-sentenced-to-six-years-in-federal-prison-for-sextortion-of-women-and-teenage-girls [Accessed 17-12-2013].

Clancy, H. 2013. Jonathan Koomey: Stop worrying about IT power consumption [Online]. *Greenbiz.com*. Available from: http://www.greenbiz.com/blog/2013/08/07/jonathan-koomey-stop-worrying-about-it-power-consumption [Accessed 16-12-2013].

Clark-Flory, T. 2013. Criminalizing "revenge porn"[Online]. *Salon.com* Available form: http://www.salon.com/2013/04/07/criminalizing_revenge_porn/ [Accessed 10-12-2013].

Cohen, J. 2012. The Patient of the Future [Online]. *MIT Technology Review.* Available from: http://www.technologyreview.com/featuredstory/426968/the-patient-of-the-future/ [Accessed 06-12-2013].

Cotter, P. & McGilloway, S. Living in an 'Electronic Age': Cyberbullying Among Irish Adolescents. *Irish Journal of Education*, 39, pp. 44-56.

Crisp, R. 2013. Well-Being [Online]. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Summer 2013 Ed. Available from: http://plato.stanford.edu/entries/well-being/ [Accessed 08-12-2013].

Cybulska, B. 2007. Sexual Assault: Key Issues. *J R Soc Med*, 100(7), pp. 321–324

Dement, W.C. & Mitler, M.M. 1993. It's Time to Wake Up to the Importance of Sleep Disorders. *JAMA*, 269(12), pp. 1548-1550.

Deneulin, S. 2002. Perfectionism, Liberalism and Paternalism in Sen and Nussbaum's Capability Approach. *Review of Political Economy*, 14 (4). pp. 497-518.

Eichorn, K.2013. Lovers Beware: Scorned Exes May Share Intimate Data And Images Online [Online]. *McAfee*. Available from: http://www.mcafee.com/us/about/news/2013/q1/20130204-01.aspx [Accessed 10-12-2013].

Eisner, A. 2010. Is Social Media a New Addiction? [Online]. *Retrevo Blog*. Available from: http://www.retrevo.com/content/blog/2010/03/social-media-new-addiction%3F [Accessed 17-02-2014].

European Commission. 2014. EU proposes responsible trading strategy for minerals from conflict zones [Online]. *Press Releases Database.* Available from: http://europa.eu/rapid/press-release_IP-14-218_en.htm

European Union Agency for Fundamental Rights. 2012. *Hate crime in the European Union*. Vienna: European Union Agency for Fundamental Rights.

FBI. 2012. Eastover Man Pleads Guilty to Bomb Threat, Child Pornography Charges. *FBI Columbia Division.* Available from: http://www.fbi.gov/columbia/press-releases/2012/eastover-man-pleads-guilty-to-bomb-threat-child-pornography-charges [Accessed 29-04-2014].

Filipovic, J. 2013. 'Revenge porn' is about degrading women sexually and professionally [Online]. *The Guardian.* Available from: http://www.theguardian.com/commentisfree/2013/jan/28/revenge-porn-degrades-women [Accessed 10-12-2013].

Finley, J.R., Brewer, W.F. & Benjamin, A.S. 2011. The effects of end-of-day picture review and a sensor-based picture capture procedure on autobiographical memory using SenseCam. *Memory*, 19(7), pp. 1-12.

Fischer, C. 2008. Feedback on household electricity consumption: a tool for saving energy? *Energy Efficiency*, 1(1), pp 79-104.

Fox, S. & Duggan, M. 2013. Tracking for Health [Online]. *Pew Research Cente.* Available from: http://pewinternet.org/Reports/2013/Tracking-for-Health.aspx [Accessed 07-02-2014].

Fox, S., Duggan, M., Rainie, L, Purcell, K. 2013. The Diagnosis Difference [Online]. *Pew Research Cente.* Available from: http://pewinternet.org/~/media//Files/Reports/2013/PewResearch_DiagnosisDifference.pdf [Accessed 11-12-2013].

Frankena, W.K. 1973. *Ethics.* Englewood Cliffs: Prentice-Hall, Inc.

Fried, C. 1968. Privacy. *The Yale Law Journal*, 77(3), pp. 475-493.

Fukuda-Parr, S. 2003. The Human Development Paradigm: Operationalizing Sen's Ideas On Capabilities. *Feminist Economics*. 9(2-3), pp. 301-317.

George, A. 2013. The Best Dash Cam. *The Wirecutter*. Available from: http://thewirecutter.com/reviews/best-dash-cam/ [Accessed 12-09-2013].

Gershman, J. 2013. California Lawmakers Retool Cyber-Revenge Bill [Online]. *The Wall Street Journal.* Available from: http://blogs.wsj.com/law/2013/08/22/california-lawmakers-retool-cyber-revenge-bill/ [Accessed 10-12-2013].

Gerstein, R.S. 1978. Intimacy and Privacy. *Ethics*, 89(1), pp. 76-81.

Gert, B., Culver, C.M., Danner Clouser, K. 2006. *Bioethics A Systematic Approach*. Oxford: Oxford University Press.

Gibbs, S. 2014. MasterCard's new phone location technology aims to kill fraud abroad [Online]. *The Guardian*. Available from: http://www.theguardian.com/technology/2014/feb/25/mastercards-new-phone-location-technology-aims-to-kill-abroad [Accessed 13-03-2014].

Giudice, K. Del. & Gardner, M. 2009. *The Message of the Pensieve: Realizing Memories through the World Wide Web and Virtual Reality*. Unpublished. Available from: http://web.mit.edu/comm-forum/mit6/papers/Delgiudice.pdf.

Google. 2014. Staying at the forefront of email security and reliability: HTTPS-only and 99.978% availability [Online]. *Official Gmail Blog.* Available from: http://gmailblog.blogspot.ie/2014/03/staying-at-forefront-of-email-security.html [Accessed 31-03-2014].

Greene, J. 2012. Digging for rare earths: The mines where iPhones are born [Online]. *CNET*. Available from: http://news.cnet.com/8301-13579_3-57520121-37/digging-for-rare-earths-the-mines-where-iphones-are-born/ [Accessed 16-12-2013].

Greenemeier, L. 2014. Online 24/7: "Life Logging" Pioneer Clarifies the Future of Cloud Computing [Online]. *Scientific American.* Available from: http://www.scientificamerican.com/article/cloud-computing-pioneer-bell/ [Accessed 13-03-2014].

Greenwald, G., Gallagher, R. & Grim, R. 2013. Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'. *Huffington Post*. Available from: http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html [Accessed 07-03-2014].

Griswold v. Connecticut. 1965. 381 U.S. 479.

Groen, J. 2014. Progressieve Marokkaanse Nederlanders in verzet tegen digitale schandpaal [Online]. Available from: http://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/3608985/2014/03/07/Progressieve-Marokkaanse-Nederlanders-in-verzet-tegen-digitale-schandpaal.dhtml [Accessed 11-03-2014].

Guardian. 2013. *Rehtaeh Parsons suicide: two charged over photos in cyberbullying case* [Online]. Available from: http://www.theguardian.com/society/2013/aug/09/rehtaeh-parsons-suicide-charged-photos [Accessed 09-09-2013].

Gunns, R.E., Johnston, L. & Hudson, S.M. Victim Selection and Kinematics: A Point-Light Investigation on Vulnerability to Attack. *Journal of Nonverbal Behavior* 26(3), pp. 129-158.

Hanson, M., Godfrey, K.M., Lillycrop, K.A., Burdge, G.C. & Gluckman, P.D. 2011. Developmental plasticity and developmental origins of non-communicable disease: Theoretical considerations and epigenetic mechanisms. *Progress in Biophysics and Molecular Biology*, 106(1), pp. 272-280.

Hayes, G.R., Hirano, S., Marcu, G., Monibi, M., Nguyen, D.H., & Yeganyan, M. 2010. Interactive Visual Supports for Children with Autism. *Personal and Ubiquitous Computing*, 14(7), pp. 663-680.

Heise, L., Ellsberg, M. & Gottemoeller, M 1999. *Ending Violence Against Women. Population Reports, Series L, No. 11. Baltimore, Johns Hopkins University School of Public Health, Population Information Program.* Takoma Park: The Center for Health and Gender Equity.

Henley, J. 2013. Ask.fm: is there a way to make it safe? [Online]. *The Guardian.* Available from: http://www.theguardian.com/society/2013/aug/06/askfm-way-to-make-it-safe [Accessed 10-09-2013].

Hertwich, E.G. & Peters, G.P. 2009. Carbon Footprint of Nations: A Global, Trade-Linked Analysis. *Environ. Sci. Technol*., 43(16), pp 6414–6420.

Hoven, J. Van Den. 2008. Information Technology, Privacy, and the Protection of Personal Data. *IN:* Van den Hoven, J. & Weckert, J. (eds.) *Information technology and moral philosophy*. Cambridge: Cambridge University Press, pp. 301-321.

Human Rights Watch. 2013. *Laws of Attrition Crackdown on Russia's Civil Society after Putin's Return to the Presidency* [Online]. Available from: http://www.hrw.org/sites/default/files/reports/russia0413_ForUpload_0.pdf [Accessed 13-02-2014].

Janevic, M.R., McLaughlin, S.J. & Connell, C.M. 2012. Overestimation of physical activity among a nationally representative sample of underactive individuals with diabetes. *Med Care*, 50(5), pp. 441-445.

Javelin Strategy & Research. 2013. 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters. Pleasonton.

Kant, I. 2002. *Groundwork for the Metaphysics of Morals*, translated by Wood, A.W. New Haven & London: Yale University Press.

Koomey, J. 2011. Worldwide electricity used in data centers. *Environmental Research Letters*, 3(034008).

Koops, B.J. & Leenes, R.E. 2006. Identity Theft, Identity Fraud and/or Identity-related Crime. *Datenschutz und Datensicherheit*, 30(9), pp. 553-556.

Kukla, R. & Wayne, K. Pregnancy, Birth, and Medicine. *IN:* Zalta, E.N. (ed.). *The Stanford Encyclopedia of Philosophy*. Spring 2011 Ed. Available from: http://plato.stanford.edu/archives/spr2011/entries/ethics-pregnancy/ [Accessed 08-12-2013].

Lahlou, S. 2011. How can we capture the subject's perspective? an evidence-based approach for the social scientist. *Social science information*, 50 (3-4), pp 607-655.

Ledger, D. & McCaffrey. 2014. *Inside Wearables How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*. Cambridge, MA, London, Washington: Endeavour Partners.

Lenhart, A. 2009. Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging [Online]. *Pew Internet.* Available from: http://ncdsv.org/images/PewInternet_TeensAndSexting_12-2009.pdf [Accessed 10-12-2013].

Lezhnev & Hellmuth. 2012. Taking Conflict Out of Consumer Gadgets Company Rankings on Conflict Minerals 2012 [Online]. *Enough Project.* Available from: http://www.enoughproject.org/files/CorporateRankings2012.pdf [Accessed 13-03-2014].

Mann, S. 2003. Existential Technology: Wearable Computing Is Not the Real Issue! *LEONARDO*, 36(1), pp. 9-25.

Marmot, M. 2003. Self esteem and health: Autonomy, self esteem, and health are linked together. *BMJ*. 327(7415), pp. 574–575.

Microsoft Research. 2014. *MyLifeBits* [Online]. Available from: http://research.microsoft.com/en-us/projects/mylifebits/ [Accessed 13-03-2014].

Mill, J.S. 1863. *Utilitarianism.* London: Parker, Son, and Bourn, West Strand.

Morozov, E. 2011. *The net delusion: how not to liberate the world*. London: Allen Lane.

Morozov, E. 2013. The Real Privacy Problem [Online]. *MIT Technology Review*. Available from: http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/. [Accessed 05-12-2013].

Murata, K. 2011. The right to forget/be forgotten. *IN: CEPE 2011: Crossing Boundaries*.

Murphy, F.C., Barnard, P.J., Terry, K.A.M., Carthery-Goulart, M.T. & Holmes, E.A. 2011. SenseCam, imagery and bias in memory for wellbeing. *Memory,* 19(7), pp. 768-777.

Nissenbaum, H. 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79(1), pp. 101-139.

NOS. 2011. *Politie gebruikt rijgegevens TomTom* [Online]. Available from: http://nos.nl/artikel/235904-tomtom-verkoopt-politie-rijgegevens.html [Accessed 02-11-2013].

Nozick, R. 1974. *Anarchy, state, and utopia*. New York: Basic Books.

Nussbaum, M.C. 1997. Capabilities and Human Rights. Fordham Law Review, 66(2), pp. 273-300.

Nussbaum, M.C. 1999. *Sex and Social Justice*. Oxford & New York: Oxford University Press.

Nussbaum, M.C. 2000. *Women and Human Development.* Cambridge: Cambridge University Press.

Nussbaum, M.C. 2003. Capabilities as fundamental entitlements: Sen and Social Justice. *Feminist Economics*, 9(2-3), pp. 33-59.

Nussbaum, M.C. 2007. *Frontiers of Justice*. London & Cambridge: Harvard University Press.

O'Hara, K., Morris, R., Shadbolt, N., Hitch, G. J., Hall, W. & Beagrie, N. 2006. Memories for Life: A Review of the Science and Technology. *Journal of the Royal Society Interface*, 3 (8). pp. 351-365.

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

O'Hara, K., 2010. Narcissus to a Man: Lifelogging, Technology and the Normativity of Truth. E. Berry et al., eds. *Second Annual SenseCam Symposium*. Available at: http://eprints.ecs.soton.ac.uk/21904/.

Oskar K. 2012. How Memoto raised $500,000 on Kickstarter, part 2 [Online]. Available from: http://blog.getnarrative.com/2012/11/how-memoto-raised-500000-on-kickstarter-part-2/ [Accessed 11-02-2014].

Pariser, E. 2011. *The Filter Bubble: What the Internet is Hiding From You.* London: Penguin Books.

Parkinson, H.J. 2014. How anti-gay groups use 'Russian Facebook' to persecute LGBT people [Online]. Available from: http://www.theguardian.com/technology/2014/feb/11/russia-violent-anti-gay-groups-vkontakte-lgbt-sochi [Accessed 23-04-2014].

Rachels, J. 1975. Why Privacy is Important. *Philosophy & Public Affairs*, 4(4), pp. 323-333.

Rawassizadeh, R. & Min Tjoa, A. 2010. Securing Shareable Life-logs. *IN: The Second IEEE International Conference on Information Privacy, Security, Risk and Trust.* Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5590506.

Rawassizadeh, R. 2011. Towards sharing life-log information with society. *Behaviour & Information Technology*, pp. 1-11.

Rebitzera, G, Ekvall, T., Frischknecht, R., Hunkeler, D., Norris, G., Rydberg, T., Schmidt, W.P., Suh, S., Weidema, B.P., & Pennington, D.W. 2004. Life cycle assessment Part 1: Framework, goal and scope definition, inventory analysis, and applications. *Environment International*, 30(5), pp. 701– 720.

Reiman, J.H. 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway. *Technology of the Future*, 11(1), pp. 27-44.

Robeyns, I. 2006. Capability approach in practice. *Journal of Political Philosophy*, 14(3), pp. 351-376.

Rose, S. 2013. Putin Signs Law Banning Gay 'Propaganda' Among Children [Online]. *Bloomberg.* Available from: http://www.bloomberg.com/news/2013-06-30/putin-signs-law-banning-gay-propaganda-among-children.html [Accessed 18-02-2014].

Ross, W.D. 2002. *The Right and the Good*. New York: Oxford University Press.

Sadilek, A., Kautz, H. & Silenzio, V. 2012. Predicting Disease Transmission from Geo-Tagged Micro-Blog. *IN: AAAI Conference on Artificial Intelligence, North America, jul. 2012.* Available from: http://www.aaai.org/ocs/index.php/AAAI/AAAI12/paper/view/4844/5130 [Accessed 11-02-2014].

SCDI. 2010. *Scottish Government Low Carbon Economy: Discussion Paper*. Glasgow: SCDI Policy Team.

Scherer, K.R. 2003. Vocal communication of emotion: A review of research paradigms. *Speech Communication,* 40(1-2), pp. 227-256)

Scott, P.A. 2014. Unsupervised Self-testing as Part Public Health Screening for HIV in Resource-Poor Environments: Some Ethical Considerations. *AIDS Behav*, 18(4), pp. 439-444.

Sellen, A., Fogg, A., Aitken, M., Hodges, S., Rother, C. & Wood, K. 2007. Do Life-logging Technologies Support Memory for the Past? An Experimental Study Using Sensecam. *IN: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* San Jose, California: ACM Press, pp. 81-90.

Sen, A. 2001. *Development as Freedom*. Oxford: Oxford University Press.

Siegrist, J. 2000. Place, social exchange and health: proposed sociological framework. *Social Science & Medicine*, 51(9), pp. 1283-1293.

Silva, A.R., Pinho, S., MacEdo, L.M., Moulin, C.J. 2013. Benefits of SenseCam review on neuropsychological test performance. *American Journal of Preventive Medicine*, 44(3), pp. 302-307.

Smeaton, Alan F. 2011. The unexpected applications of sensors: Home energy and lifestyle analysis. In: *The Internet Of Things For A Sustainable Future*, 9-13 May, Vielsalm, Belgium.

UCS. 2002. *The Hidden Cost of Fossil Fuels* [Online]. Available from: http://www.ucsusa.org/clean_energy/our-energy-choices/coal-and-other-fossil-fuels/the-hidden-cost-of-fossil.html [Accessed 17-12-2013].

Walker, S. & Grytsenko, O. 2014. Text messages warn Ukraine protesters they are 'participants in mass riot' [Online]. *The Guardian*. Available from:

http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot [Accessed 11-02-2014].

Wall Street Journal. 2013. *What They Know Mobile* [Online]. Available from: http://blogs.wsj.com/wtk-mobile/ [Accessed 03-12-2013].

Watkinson, C., Sluijs, van E.M.F., Sutton, S., Hardeman, W., Corder, K. & Griffin, S.J. 2010. Overestimation of physical activity level is associated with lower BMI: a cross-sectional analysis. *International Journal of Behavioral Nutrition and Physical Activity*, 7(68), pp. 1-9.

Weber, C.L. & Matthews, H.S. 2008. Food-Miles and the Relative Climate Impacts of Food Choices in the United States. *Environ. Sci. Technol*., 42(10), pp. 3508–3513.

Wolf, N. 2012. Amanda Todd's suicide and social media's sexualisation of youth culture [Online]. Available from: http://www.theguardian.com/commentisfree/2012/oct/26/amanda-todd-suicide-social-media-sexualisation [Accessed 23-04-2014].

Women's Aid. 2013. *National and International Statistics* [Online]. Available from: http://www.womensaid.ie/policy/natintstats.html [Accessed 10-12-2013].

World Health Organization. 2011. *Global Health and Aging* [Online]. Available from: http://www.who.int/ageing/publications/global_health.pdf [Accessed 27-03-2014].

Yong Tao, S.D. & Martinez, A.M. 2014. Compound facial expressions of emotion [Online]. *IN:* Heeger, D.J. (ed.) *Proceedings of the National Academy of Sciences of the United States of America*. Available from: http://www.pnas.org/content/early/2014/03/25/1322355111.abstract [Accessed 23-04-2014].

Becoming a lifelogger

7 Autonomy

Introduction

Following the discussion of the effect of lifelog technology on autonomy in Chapter 5, this chapter will focus on the conditions under which prospective lifeloggers become lifeloggers. Thus, it concentrates on autonomy on the level of execution. The decision to become a lifelogger is materialised with the purchase of a lifelogging device, such as the Narrative Clip, or the installation of a lifelogging application that transforms an existing device into a lifelogging device, such as Saga for the smartphone, and by deploying these technologies for the purposes of lifelogging.

Lifelog technology can greatly affect lifeloggers and others around them so it is important that the decision to become a lifelogger is an autonomous one made by the lifelogger herself. The potentially negative effects of *using* lifelog technology on privacy, autonomy, and the good have been discussed expansively in previous chapters. Lifelog technology can be designed without due care for these three matters. Nonetheless it may be argued that these infringements are inconclusive to argue for a moratorium on the further development of lifelog technology when they are judged as acceptable by prospective lifeloggers. In a situation where a competent person has decided freely with sufficient understanding that despite these possible harms, the use of the technology is in his best interests, the argument to halt the further development of lifelogs becomes less persuasive.[148] After all, respect for autonomy prescribes that one ought to respect autonomous decisions.

The conditions under which one becomes a lifelogger have yet to be discussed in more detail within the academic debate on lifelogs. As the principle of respect for autonomy has already been discussed in the chapter on autonomy, there is no need to provide a detailed account of it again. However some conditions for autonomous decision-making are briefly explained. After this, the ways the conditions might be compromised are examined, which is followed by recommendations to alleviate concerns.

---

[148] This does not mean that issues with autonomy, privacy and the good should be ignored once someone chooses to lifelog. The *prima facie* duties of developers to care for autonomy, privacy, and the good of the lifelogger and others remain unaffected. Indeed, developing lifelogs while failing to respect autonomy, privacy, and the good remains ethically undesirable.

7.1 Autonomous decision-making

In the chapter on autonomy, two conditions for autonomy were provided; namely, one has to (1) have sufficient understanding and (2) be free from controlling influences. The first condition will be further expanded by separating it into two separate clauses; namely, (1a) disclosure and (1b) having the competence to deliberate. Both the necessity of the availability of appropriate information, as well as needing to have the mental capacity for deliberation are undisputed requirements for autonomous decision-making.

1a) Disclosure: Disclosure of relevant information is an undisputed condition for understanding the situation at hand, and thus, autonomous decision-making. This condition requires more than solely providing information but the information needs to be accurate, comprehensible and suitable for the purposes intended. Indeed, too many technical details or jargon can impair decision-making by making the decision unnecessarily complicated. As full disclosure of all relevant information in a manner that is understandable to all is often impossible, e.g. some situations are too complex and offer too many details to explain, some standard is applied to determine if the person is offered sufficient information to understand the decision. In medical ethics three standards prevail that also have resonated in law, namely, a professional standard (based on what the professional community considers adequate disclosure), a reasonable person standard (based on what information is pertinent or material for a reasonable person to make a decisions), and a subjective standard (based on what information a specific person needs) (Beauchamp & Childress 2009, 122-123).[149]

1b) Competence: Competence is a concept predominantly used in medical ethics. However having the mental skills for deliberation is equally important to autonomous decision-making outside of the realm of medicine. It is evident that without the capacities necessary to make an autonomous decision, one cannot be autonomous even when all other conditions for autonomous decision-making are present. Competence can be considered to consist of several different capacities such as: the person is capable to understand information presented to them; the person is capable to evaluate information based on his own values and situation; the person is capable to understand the nature and significance of his choices.[150] Competence exists on a spectrum: is gradual and intermittent as the capacities of the person

---

[149] The body of work in medical ethics on standards for disclosure can also inform issues with standards for technology because there do not seem to be decisive reasons that the standards identified for medical ethics cannot be applied to or considered for technology.

[150] There is some controversy over the precise capacities a person ought to have (Beauchamp & Childress 2009, 113; Charland 2011). These capacities provided serve as an example and are not meant as a conclusive list.

can vary depending on the situation and over time, e.g. one's capacity of understanding information can be temporarily impaired and one's ability to understand information can differ in time. There is a minimum level of competence below which one is considered incompetent to make a decision in a given situation. The level of competence required for a decision is commensurate with the complexity of the situation.

2) Being free from controlling influences: The condition of being free from controlling influences can be impaired in several ways. Two of them are relevant to this discussion, namely, (a) coercion and (b) creating a situation in which the offer unfairly or undesirably curtails the options. Coercion is a threat aimed to induce one to behave differently than one would have without the threat being there. Sometimes the threat is implicit. This could be the case when one is encouraged to take part in a research undertaken by one's superior and when one has reasons to believe that refusing to participate would impair one's relationship with him (Beauchamp and Childress 2009). There is a second category, namely, when the offer – in this case the introduction of the technology – unfairly or undesirably curtails one's options (Eyal 2011). As explored below (*7.2.3.3 Positional goods*) curtailing people's options can be considered unfair or undesirable if a situation is created in which the options available to one have become less favourable than before the introduction of the technology.[151] As stated in the chapter on autonomy (*5.1.1 Core components of autonomy*), absolute freedom from controlling influences is unattainable (and maybe even undesirable). However, again, it is possible to draw attention to predicted negative effects.

7.2 Challenges

In the next sections, issues with disclosure, competence, and being free are discussed. This section is divided into three parts corresponding with the three conditions for autonomous decision-making.

---

[151] The introduction of a technology is not necessarily an advancement of one's opportunities. It may seem that offering a technology means that one's options are necessarily increased. After all, before the technology one did not have the option to purchase the technology. For some technologies this may so. An automated coffee maker does not disrupt society. It merely expands the options of the consumer to buy an additional product. However some technologies can change society profoundly and curtail the opportunities people have. Arguably as discussed below, lifelogs could be such a technology.

7.2.1 Disclosure

A researcher developing the SenseCam once described the device as "a black box data recorder for the human body" (Schofield 2004), which is an apt description for several reasons. In the most ordinary sense it has the appearance of a black coloured box. The researcher, however, seems to refer to its functioning, which shows similarities to a device originally used in aviation.[152] The 'black box' in an airplane is a flight recorder that stores the recordings of the conversations of the pilots and information about controls and sensors. These data can be helpful when investigating an accident. Similar to the black box providing information about a flight, the SenseCam can provide information when examining events from the past of the lifelogger.

The concept of the 'black box' has another relevant connotation which will be the subject of inquiry in this section, namely, that of an intricate system or device which internal workings are concealed or not readily understood. Lifelogs are also a black box in the latter sense. In contrast to some instruments, such as knives, headphones, or books, in order to understand the lifelog technology, one would need to be handed accurate, sufficient, and comprehensible information about its functioning. There is a myriad of information that can be obtained from lifelog data that can be altered, accessed or distributed by others. It is largely dependent on the discretion of the developers – besides the technological and legal limits to what is possible – to determine the information that is retrieved within a lifelog and the control and information the lifelogger has over the storage, access and distribution of data. Only with expert knowledge one might be able to discover processes that were hidden by the developers. It is by no means certain that the lifelogger is indeed properly informed about the functioning of lifelog devices. Important information can be missing, or the information includes too much jargon to be properly understood. At other times the information offered is too non-specific (*4.2.3.2 Concerns regarding access and distribution of information*). Besides informing the lifelogger about the content and functioning of its devices and applications, lifelog companies have to disclose pertinent information about concerns relevant to privacy, autonomy, and the good.

1) Information about privacy-related concerns is important as to maintain the lifelogger's privacy for which control was an integral element. As discussed in the chapters

---

[152] These devices are currently also widely used for other modes of transportation such as automobiles, ships and locomotives).

on autonomy and beneficence, the distribution and access of data can have ramifications for the good and autonomy of the lifelogger.

Privacy policies, one of the most basic instruments to protect consumers, are not always offered to consumers as discussed before (*4.2.3.1 Concerns regarding control over the creation of data*). Smartphone applications, which are expected to become an important element to lifelog technology that can access and handle terrific amounts of personal data, can lack this basic instrument to inform people about privacy-related information. Consent procedures, if present, can also fail to reach satisfactory standards for disclosure. Blanket permissions demanded from users before they install an application on their smartphone or browser can be formulated so broadly that the users cannot have a clear idea of what they are actually consenting to (Brandom 2014; Talbot 2014).[153] Instead of protecting the consumer, these permissions rather seem to function as a fig leave that allows corporations to further disregard privacy. Corporations can even wilfully disclose erroneous information. Technology giant Facebook misinformed their users by offering the option to remove photos while the data remained on their servers (the direct link was removed from user-profiles but the link to the data remained intact for over a year); an issue that has now been resolved (Cheng 2012). In other cases, the companies are legally prevented from sharing information about data disclosures. Currently, a few prominent technology companies are pressing for more transparency about demands by governments for access (Wyatt & Miller 2013).[154] However, it should be possible for lifelog companies to inform their users that confidentiality is subject to legal limitations and that their data can be subpoenaed by government agencies.

---

[153] One issue is that people may not be aware of the amount and magnitude of data being shared. Smartphones are notorious for gathering and distributing personal information without clearly communicating it to their users so that even advanced users struggle to grasp the level and comprehensiveness of information distributed (and in some cases accessed by third parties such as governmental organisations or other companies) (Glanz, Larson & Lehren 2004).

[154] The falling trust of consumers seems to be a rather cynical explanation of their want for this transparency but no other explanation seems that apt as corporations have shown little interest in privacy before. More information on this initiative can be found on: http://reformgovernmentsurveillance.com/. Indeed, the NSA surveillance programmes are estimated to cost from $22 to $35 billion (Castro 2013) to up to $180 billion (Staten 2013) by 2016 due to customers (consisting of a wide variety of customers such as private individuals, companies, and governmental) distrust. The CEO of Cisco, John Chambers, wrote the 15th of May 2014 a letter to the US president stating that the actions of the US government "undermine confidence in our industry and in the ability [of] technology companies to deliver product globally." (Letter is available from http://recode.net/2014/05/18/in-letter-to-obama-cisco-ceo-complains-about-nsa-allegations/ [accessed 23-05-2014])

2) Some autonomy-related concerns also ought to be explained to the prospective lifelogger. Autonomy concerns related to privacy will already be addressed in the privacy policy, but there are remaining issues that require clarification. In the chapter on autonomy, some risks to autonomy posed by lifelog technology were identified. One is that information retrieval and lifelog content can be made to serve other purposes than just providing lifeloggers with a medium to search for information about their past. Companies offering applications or devices may use lifelogs to market their product. Using lifelogs to market a product or guide behaviour is not unethical *per se* –e.g. using lifelog to improve the health or fitness levels of the lifelogger – and can even be ethically desirable. However, the purposes for which lifelogs are used can affect the content presented to lifeloggers and, subsequently, their understanding about themselves and their environment. Adequate disclosure beforehand can function as an instrument to prevent future manipulation when the technology is used.

3) Lifelog technology can cause harms that may require clarification before one becomes a lifelogger. The novelty of lifelog technology makes an explanation of potential harms even more urgent. The possibility that the prospective lifelogger would be unaware of these harms is greater when consumers are unfamiliar with the technology than when consumers are thoroughly familiar with the functioning of the device. In the chapter on beneficence, it was mentioned that the use of lifelogs could negatively affect people suffering from certain mental disorders (*6.2.2 Bodily Health*). If this turns out to be the case, developers need to inform prospective lifeloggers. The ethical duty to mention the benefits expected from lifelogs is less urgent as people are less likely to avoid lifelog technology when lifelogs are more beneficial than the lifelogger initially expected, i.e. there are no issues with autonomy expected, as more benefits will not change their choice to begin lifelogging.

Conclusion: A failure to inform the lifelogger properly would hinder understanding of the situation at hand, which is one of the conditions for autonomous decision-making. Therefore it seems necessary for companies that offer lifelog services and products to explain comprehensively and comprehensibly that which is of interest to the lifelogger. Little seems more important for lifeloggers than the risks and benefits to privacy, autonomy, and the good stemming from lifelog technology. Corporations that offer sufficient and comprehensible information about their lifelog technology can satisfactorily meet the standard for disclosure. Current practices, however, do not seem overly optimistic that this standard will in fact be met.

There are several standards to determine what information needs to be revealed and in what form.[155] The technology sector is dispersed and relatively unregulated compared to the healthcare sector with companies offering services and product for many different reasons in many different areas and jurisdictions which makes a widely carried consensus about a professional standard doubtful. Indeed it is questionable if guidelines by the industry would result in satisfactory standards at all. Companies could systematically undervalue the importance of certain aspects or there could be a disparity between what professionals and consumers consider relevant. The professional standard by itself seems to undermine autonomy by imposing a preconceived standard determined by experts instead of letting consumers decide on the pertinence of information disclosed (Beauchamp & Childress 2009). Indeed, what experts think that is or ought to be considered pertinent is irrelevant. Paramount is what consumers think is important for their choice. The subjective standard is impractical. Technology is often purchased with brief interpersonal contact and sometimes even without face-to-face encounters. The preferred option (or the least bad option) is to use a reasonable person standard in which the pertinence of information is measured by the value a reasonable person would attach to the information in deciding whether to use the technology. As a definitive idea of what constitutes a reasonable person is missing, there are practical, conceptual and moral difficulties to this standard. However these issues are not as decisive as the moral and practical issues associated with the subjective and the professional standard.

7.2.2 Competence

The prospective lifelogger requires sufficient competence to grasp the information presented to him and the nature and significance of his choice when presented with the decision to become a lifelogger. The choice to lifelog is often complex as it invokes a weighing of multiple, possibly conflicting interests. The prospective lifelogger has to decide whether lifelogging is worthwhile.[156] The mental skills that are required to make an autonomous decision about becoming a lifelogger depend on the characteristics of a particular lifelog technology. A lifelog company that increases user-friendliness and avoids social, moral, and

---

[155] These standards are taken from bioethics as bioethics has had a tradition of dealing with matters concerning autonomous decision-making and is arguably more advanced in this field. This paragraph is largely informed by Beauchamp and Childress (2009).

[156] Indeed, even when already chosen to lifelog one need competence to decide whether lifelog information is indeed useful in a particular situation. As discussed before (*5.2.1.1 Biases*), lifelog information is not always suitable to increase understanding. Besides benefiting from the use of lifelog, lifeloggers also require some competence to use the lifelog discretely. Some situations might better not be lifelogged. The lifelogger will have to continuously decide whether he should be lifelogging and if the information from the lifelog is useful something which has been discussed before (*5.2.1.3 Overload of information*).

legal difficulties also reduces the mental capacities required of those that need to make the decision about becoming a lifelogger, e.g. avoiding issues with privacy in design would reduce the need for the lifelogger to balance the risks for his privacy against other benefits.

This kind of technology - and there do not seem to be any reasons to suppose that this would be different for lifelog technology - is typically available for mass consumption and purchased without the kind of social contact or procedures to establish consent preceding non-urgent medical procedures. Therefore it seems impossible to establish competence on an individual basis as basic issues such as who would be the one to establish competence seem unlikely to be solved. An unsophisticated measure to ensure that most of the population is indeed competent is to set age restrictions either on particular functionalities, or lifelogs as a whole. In general, during childhood, one is less competent to make intricate choices, e.g. children often have a limited capacity for self-control and are susceptible to peer pressure (Schurgin O'Keeffe & Clarke-Pearson 2011). Their capacity to make autonomous decisions is generally improved over time. Facebook has limited their service to people that are at least thirteen years old, a requirement ultimately enforced by law rather than wholeheartedly embraced by the company.[157] This is a coarse instrument as it could both include individual persons that are incompetent and exclude those that are competent. There may be other groups equally unfit to make such decisions (e.g. those suffering from particular mental illnesses). Another issue is that mental development differs between individual persons. Some children develop the mental skills necessary for complex decision-making at earlier stages than others while others develop relatively late or do not develop their capacity for complex decision-making at all. The appropriate minimum age ultimately depends on the design of the particular lifelog and will not be subject of this inquiry.

There may also be another disadvantage associated with excluding certain age groups. Even though Facebook restricts access to children under thirteen, many of them have become a member with the help of their parents. However, as Facebook is not designed to accommodate people within this age bracket it offers insufficient tools to support the needs

---

[157] In the US, the Children's Online Privacy Protection Act (COPPA), a federal law, regulates the privacy and collection of person information online from children under the age of thirteen (Children's Online Privacy Protection Rule 1998). Mark Zuckerberg, cofounder, CEO and chairman of social networking site Facebook, has announced to challenge this law but has not yet done so (Bazelon 2011). The US Federal Trade Commission has set the limit to under thirteens because they are, according to them, most vulnerable to marketers and less likely to understand security and privacy risks (Federal Trade Commission 2013).

and interests of these children or to the carers to protect their children (Boyd et al 2011).[158] Regarding lifelogs, another suitable option might be to place age-restrictions on particular functionalities instead of on the whole lifelog, such as disenabling the feature for children to retrieve photos containing information about others, and create a user-interface more suitable to their age bracket.

Conclusion: The responsible use of lifelogs might require capacities that some people will lack. The developers can anticipate this issue by trying to minimise the complexity of lifelog devices and applications. A pragmatic measure to protect a group of which many may not (yet) be competent is to set age restrictions for certain features and adjust the user-interface. Age restrictions will not help people who have intellectual disabilities. An indirect measure to protect people with intellectual disabilities is to have information about the functioning of the devices or applications readily available for carers or guardians. A more substantive measure is to allow the guardians or parents to restrict access to certain features manually when people in their care show an inability to deal with these features.

7.2.3 Being free

There are four autonomy-limiting factors when deciding to become a lifelogger, namely: (1) governmental pressure to lifelog; (2) pressure by one's social environment to control the behaviour of the lifelogger; (3) the benefits lifelogs provide as a positional good; (4) and society inducing the use by embedding them into the fabric of society.

7.2.3.1 Governmental pressure

Allen (2007) warns that one should avoid that lifelogs become a symbol to signify that one has nothing to hide and thus create social pressure to keep a lifelog. According to her, "[n]o one should be suspected for not keeping a lifelog" (Allen 2007, 74). However, it is difficult to see how the use of a lifelog in fact would turn into a signifier of innocence towards government agencies. For one, it seems necessary for practical reasons that the technology is used by an overwhelming majority to such a degree that not using lifelogs becomes noticeable. In a community in which only a few people are lifelogging, the non-lifeloggers do not raise suspicion. Moreover, it seems necessary that lifelogs need to be embedded into that community to the extent that refraining from using them would require large sacrifices;

---

[158] The pressure exerted by children on their parents to allow them to use lifelogs will most likely be lesser than the pressure to use social networking sites such as Facebook. These social networking sites are part of the children's social life by providing access to their circle of friends. Lifelogs do not (necessarily) function as a social platform which might alleviate the pressure on parents.

hence, a strong motive for not using them must be present to explain why the individual refrains from using the lifelog, e.g. hiding criminal or otherwise immoral activities.

However, even if these conditions are fulfilled, not using lifelogs might not raise suspicion. Take for example another device that creates huge amounts of personal information and make those available to government agencies: the cellular phone. Cellular phones are dissimilar in many ways from lifelogs, but similar in at least one important way as they can create a trove of data that can be used by authorities to incriminate people. Solely by using metadata, which is transactional information, a comprehensive picture of the social environment and behaviour of the owner of the cellular phone can be revealed (Greenwald 2013).[159] Even physical movements and relationships could be tracked solely based on location information obtained through triangulating the distance of a cellular phone to cellular towers (Gellman & Soltani 2014). Indeed, this is all possible using metadata without even accessing communications - the actual content of conversations or text messages. The latter will reveal even more information about the individual. Thus, for a criminal, it would be imprudent to use or continuously use the same mobile phone. In addition, it seems unlikely that lifelogs will have a significantly higher penetration than cellular phones as in certain countries penetration of cellular phones was already 100% as early as 2005 (Commission for Communications Regulation 2005). However, it seems unlikely that many people have been suspect *solely* because they *refrained* from using cellular phones. Suspicion is raised by the manner in which people use their phone in combination with addition circumstances. Also for lifelogs it will be the manner in which one uses the lifelog that indicates malice or disobedience rather than the choice as such to refuse to use lifelog technology at all. Some irregularities are difficult to explain; it can be considered suspect in particular contexts when someone throws away their cellular phone or stops the security cameras and erases the tapes. Similarly it will raise suspicion when a lifelogger uncharacteristically stops logging or deletes information at times of (potential) mischief. These situations seem only to raise suspicion under conspicuous circumstances and do not indicate any form of pressure to become a lifelogger.[160] Indeed, it seems more likely than one becomes suspected because one uses a

---

[159] Because metadata are not communications they do not require individual warrants, which makes metadata especially problematic (Greenwald 2013).

[160] In the case of the former Taoiseach of the Republic of Ireland Bertie Ahern, the fact that he had no current account with a bank early 1990s as a minister of finance in conjunction with him being unable to account for his finances raised suspicion of misbehaviour (Gray 2008). However, in this case there were additional reasons that raised suspicion. The fact that Ahern was not using a current account only raised eyebrows because he was a minister of finance and had large sums of cash in his possession that could not be accounted for.

lifelog than that one would be suspected because one refrained from using a lifelog. Recent revelations show that intelligence bureaus seem to reap the low-hanging fruits, i.e. people are targeted because they use services that make digital information about them available. The US National Security Agency (NSA) had a programme in which data from people within three degrees of separation from a terror suspect is an example of that (Ackerman 2013). It is likely that persons are targeted solely because they are a member of a social network and that they would be free from suspicion if they had had no online presence.

There is a related issue regarding lifelogging to prove one's innocence. The aforementioned Hasan Elahi holds something similar to a lifelog, namely a lifeblog – a lifeblog is a public website containing manually uploaded digital information to provide insight into one's life to others - in order to protect him from a threat posed by the FBI (O'Hara, Tuffield & Shadbolt 2009; TED 2011).[161] The FBI suspected him of terrorist activities and required information about his daily goings-on. By setting up a blog he created a medium through which the FBI can access information they would otherwise have requested from him directly. Moreover, by keeping this information Elahi made sure that he could provide them with the information they sought as he was afraid that he could not satisfy their need for personal information. The artist Ai WeiWei did something similar in the People's Republic of China when lifecasting – making data in real-time available on the Internet. After repeated encounters with government officials, also he wanted to show that his behaviour was innocuous.[162] These individuals chose to proactively prove their innocence because they were actively and openly targeted by the authorities.

---

[161] There are multiple motives for Elahi to share this information. One of them is to diminish the power of intelligence service. If people would start sharing information on a broad scale like he does, sharing would, if broadly adhered to, lead to a devaluation of personal information for intelligence services (TED 2011). According to him, those secret services are dependent on the scarcity of information, which depend on a exclusive access to information. This premise is questionable. In fact, the scarcity and value of information is dependent on the ability to infer conclusion from data. Therefore, the determining factor in assessing the value would be the ability to mine the data. As recent revelations have shown, at least the US government has invested ample funding in order to find ways to process this data. In addition, they already have an immense amount of information. Moreover, Elahi's creation is a work of art. Besides the aesthetics, one can consider his work is a powerful statement to highlight current injustice more so than any practical or just solution. His website is available from: http://trackingtransience.net/.

[162] Although arguably in his case, the fact that he showed his behaviour to be innocuous angered the authorities for some reason and they removed the lifecast. In addition, the lifecast (a digital stream of information made available for an audience in real-time) protected him as any abuses would be visible as well as informed others that worried about his well-being. As mentioned before, the proactive move of citizens to provide information without being explicitly requested is accepting the burden of proof whilst it should lay firmly with the authorities. This touches fundamental values and rights such as the presumption of innocent and the right to

Potential pressure from the politically environment in which one is situated to keep a lifelog is not by itself a reason to consider the decision to become a lifelogger compromised by lifelogs. Prospective lifeloggers could autonomously decide that they prefer to lifelog above facing threats arising from the political environment in which they are situated. The interests of Elahi and WeiWei would not have been served by denying them access to these technologies. Indeed, in the case of WeiWei these technologies were removed by government officials who considered the lifecam undesirable. In that particular situation, the issue that must be addressed is the political environment. Hence, this pressure by itself is insufficient to consider the freedom to lifelog unfairly or undesirably compromised by the existence of lifelog technology.

However, this usage of lifelog technology could create moral hazards. People who start lifelogging to show their innocence to governments could inadvertently facilitate further state surveillance worsening this issue for others. When lifelogs are used on a broad scale it seems likely that the authorities will try to obtain structural access to this source of information, for example by weakening encryption and building in backdoors. Currently some governments show little reticence in accessing personal information as has been shown in the revelations about the NSA and the UK Government Communications Headquarters (GCHQ) (Ball, Borger and Greenwald (2013) or Gellman, Tate and Soltani (2014) but the examples are abundant and can be found throughout this dissertation). Some individuals will only be targeted because information about them has been made digitally available, potentially jeopardising their well-being and/or safety. The fact that citizens often be unaware that their data have been searched allows governments to lower the criteria to investigate people's daily goings-on. In contrast to physical searches, searching data requires a lot less time and resources from both citizens as well as government officials. The burdens associated with surveillance become less apparent.

Nonetheless, it seems unlikely that a large number of people would have the same incentives as WeiWei and Elahi to begin capturing information. Currently, for most people the threat posed by the authorities is distant as they will often be unaware of being targeted. Therefore it is unlikely that protection against authorities will become a strong motivation for many people to lifelog. In addition, one already leaves a trail of personal information that can

---

privacy. Obvious in these particular cases, their websites can be interpreted as a multifaceted statement against authorities beside it being just a way to protect them. However, as a mechanism to curb authoritarian power, this solution falls short.

be made available to the authorities (something which already has been extensively discussed in the chapter on privacy) which would make the additional need for lifelog information minor. Unless one wants to protect oneself against potential arbitrariness of government agencies by collecting evidence that one is innocent, then keeping lifelogs for this purpose would be rather superfluous. In the latter case, lifelogs would again be a solution to a problem rather than a cause; in other words, they would offer an advantage instead of worsening the situation. Furthermore, despite the state surveillance currently present there does not seem to be evidence that many people feel the need to maintain an archive with personal information to disprove possible allegations.

Conclusion: In summary, it seems unlikely that many will feel compelled to lifelog, because they consider it necessary to show their innocence or to protect themselves against overzealous government agencies. In addition this pressure is not (primarily) caused by lifelog technology but rather is the result of the political environment and aggravated by the fact that there are already vast streams of digital data available to governments for surveillance. Hence, lifelogs did not cause a situation in which prospective lifeloggers are undesirably or unfairly pressurised into lifelogging. Therefore the desired course of action would be to reform the political environment instead of demanding a halt to the further development of lifelog technology. An overhaul of the system is a long and demanding process so lifelogs could provide a short-term solution to address urgent needs.

7.2.3.2 Social pressure

Lifelog technology can be enforced by people in one's social environment to control the behaviour of the lifelogger. For example, parents could force their children to lifelog so that they can keep track of their daily goings-on. Potential targets could be girls who are already allowed little freedom and whose behaviour can affect the family honour.[163] The fact that lifelogs can be enforced within a family makes it more difficult to protect potential victims against the pressure exerted upon them. The force applied would be less visible to outsiders than when a corporation or an authority imposes it on their staff or citizens.

The scope of this issue depends largely on the social acceptability of requesting access to lifelogs. Demanding access to one's lifelog can be seen as equally invasive as demanding access to one's diary or one's private messages on one's social network. Often demands to

---

[163] Additional restrictions in freedom could even be dangerous. Already girls in the Netherlands from Turkish, Hindu or Moroccan descendent have a higher rate of suicide partly because of limited freedom of choice and pressure to protect family honour (Felten & Pierik 2011).

read a diary or check private messages are judged an inappropriate or unjust infringement of one's privacy. People are often allowed by their social environment to keep these things private. It seems probable that demanding access to someone's lifelogs will be considered equally disproportional as the lifelogger would be left with very little privacy. The most likely victims of this kind of pressure from their social environment are those that are already under close scrutiny and already have little freedom.

There is a more subtle way in which people can be pressurised to lifelog by their social environment. People may consider it someone's responsibility to lifelog. Lifeloggers can be informed about many aspects and so can prospective lifeloggers if they choose to lifelog. The fact that prospective lifeloggers could have been informed can render them vulnerable to accusations of negligence or imprudence.[164] Suppose someone contracts a disease possibly caused by his lifestyle or that could have been prevented with a healthy lifestyle. This person could have difficulties maintaining that he is not to blame because he may have failed to properly inform himself about the risks he took when he did not use a lifelog. Indeed, he could be blamed for his negligence.

The social pressure to use a lifelog to avoid blame can be undesirable for three reasons. The first is that the non-lifelogger may consider lifelogging not to be in her best interests. The second is that there may be good reasons not to begin lifelogging that, in balance, make lifelogs ethically undesirable, such as threats to one's privacy, autonomy and their well-fare. The third is that lifelogs can gather information about so many aspects that people could become held responsible for matters ever so trivial (*5.2.1.3 Overload of information*). The obligations to act in a particular fashion assigned to people become unfairly burdensome.

Conclusion: There seems to be no way to prevent these issues from occurring. Being directly coerced by one's social environment into lifelogging is a violation of autonomy. The direct imposition of the use of lifelog technology by one's social environment such as friends

---

[164] The increased ability to assign responsibility is not necessarily undesirable. It can have personal societal advantage because people are less able (and maybe likely) to place the blame on a cause external to them. Moreover, increasing the ability to assign responsible can serve both as a deterrent for bad behaviour as well as a motivator for good behaviour, which can be beneficial for the individual and her environment (and therefore, on a greater scale, for the whole of society). Indeed, when responsibility can be assigned, there may be ways to allocate the costs of these misbehaviours more fairly. It is worrying when the lifelogger fails to properly value other aspects of the good that are not captured by lifelogs. Moreover, the fact that lifelogs might capture details can lead to disproportional attention to details. People who, without lifelogs, take appropriate care of their health might be blamed for failing to address minor details that seem negligible with regard to the good.

and family would be disconcerting as it would leave one with very little privacy. However prevailing social norms make it unlikely that this would happen often. There seems to be no obvious way to prevent the other issue, namely pressuring people to lifelog by accusing them of negligence when they do not lifelog.

7.2.3.3 Positional goods

The third manner in which the existence of lifelogs could exert pressure upon people to begin lifelogging is the advantages the technology provides towards others who do not use it. The lifelogger might need fewer resources and less time to retrieve information about the past than others who lack access to this kind of digital archive. Having this much information could prove beneficial in some contexts; for example, when it is advantageous for one's profession to have a precise account of the person's activities. The fact that the lifelog enhances a particular skill is not idiosyncratic to lifelogs. After all, society is permeated with technology that enhances certain specific capabilities to some extent: phones allow people to communicate over further distances; cars and airplanes to travel faster; and the WWW to access information with fewer resources. Nonetheless lifelogs might undesirable or unfairly curtail one's options.

Lifelogs can be "positional goods" (Bostrom & Roache 2008, 10) which are goods whose value for the user depend on others not having access to them. It is quite possible that in some contexts the main reason to use a lifelog is to obtain an advantage over someone else. The situation could be as follows. Employee 'X' uses a lifelog because he considers they give him an edge on other workers within his highly competitive company. Because he is the only lifelogger, the issues experienced by him and others with regard to privacy are relatively minor. As a result of using the lifelog, he has been more meticulous and productive. The company is highly competitive and both possibilities to be fired as well as promoted are present. Employee 'Y' feels she has to do the same because she cannot risk being fired and is aiming for promotion. To maintain their competitiveness, most employees within the department begin lifelogging. The advantage they have over each other is cancelled out with the widespread use of lifelogs. Whilst the advantage has disappeared for them, the issues with privacy have augmented. Unfortunately, it is not possible for them to return to the situation before the use of lifelogs, because they would lose ground to others and the company is now anticipating the use of lifelogs. The situation has only worsened for the employees.[165]

---

[165] The situation shows similarities to the prisoner's dilemma within game theory.

In contrast to many other technologies, lifelogs actually have the potential to gather information about other persons. Lifeloggers can use this information to their advantage.[166] For example, if person 'X' records and stores his conversations, he will have a vast archive of information about person 'Y' with whom he has regular conversations. When 'Y' has no recordings, it will leave her vulnerable to the discretion of 'X' who could decide (at any moment) to share information about her outside her control. He could even edit information and present this as favourable to him and/or unfavourable to her. By also keeping a lifelog she has recordings of her own to counter or correct assertions and that can function as a deterrent to the sharing of information.[167] Either of these options, namely, holding a lifelog or relying on the other, can be undesirable as one often does not want to become dependent on the discretion of someone else while the usage of lifelogs can have negative implications for privacy, autonomy, and the good.

Issues with justice regarding this issue – i.e. that some people would have access to the technology and its advantages because of their social economical position and others have not - seem mostly avoided as lifelog technology will most likely be widely available to most. The cost of equipment needed to create a lifelog will likely further decrease (with the lower costs for sensors, processing power and storage). Indeed, the sale of smartphones, which are potential lifelog devices, has exceeded sales of feature phones in 2013 (Gartner 2013).[168] In India the market for smartphones grew by 229% in the third quarter of 2013 compared to the results from a year ago (Mansfield 2013). Even in the poorest inhabited continent, Africa the shipment of smartphones increased by 21.5% (IT News Africa 2013) and the African market is predicted to grow from 79 million consumers at the end of 2012 to 412 million by 2018 (Informa 2013). Indeed, it seems unlikely that many people, who would need to use lifelogs to remain competitive with others in their environment, would be structurally denied access to lifelog equipment.

---

[166] The same applies to institutions which may obtain more information about the individual than the individual itself has. After all, third parties such as governmental bodies can have incredible resources to gather data about the individual. This leaves the individual vulnerable when it has not the same amount of information to counter assessments. This is a similar argument to the one made above (*7.2.3.1 Governmental pressure*) about the inconvenience experienced by people not lifelogging when they are confronted with an institution that is accusing them or has in any way registered erroneous information.

[167] As was shown in the discussion on the results of the literature review (*3.3.3 Imposed identities*), the possibility to restore one's image is not always possible, which render this by no means a conclusive solution to the problem. In terms of game theory, this dilemma would be called the strategy of Mutually Assured Destruction.

[168] A 'feature phone' is typically a low-end phone with fewer features than a smartphone.

Conclusion: Lifelogs can be positional goods, because they can offer benefits to the lifelogger that do not occur when other people also lifelog. This issue can be reduced by avoiding that lifeloggers can store data about others within their lifelogs. Moreover the weight of this issue can be reduced by minimising harms to privacy, the good and autonomy. After all, technologies that advance skills are usually judged acceptable.

7.2.3.4   Embedding in society

Another form of societal pressure is society commanding the use of lifelogs by embedding them into the fabric of society.

Technology can change society. Take for instance the automobile. Arguably, people's lives changed as a consequence of the widespread adoption of cars. With an automobile one could bridge greater distances enabling one to live farther away from friends, family, employers, and public facilities. Even the physical environment changed with the construction of infrastructure such as roads suitable for cars. The widespread use of cars has complicated daily life for those that do not have access to this technology especially in remote areas. The choice whether to obtain a driver's licence has become one that has far reaching implications. Often this kind of pressure arising from the widespread use of the technology is considered morally acceptable, especially when the technology offers more benefits than harms. Few people argue against the use of cars because they changed society and made functioning in daily life more challenging for those without a driver's licence. People argue against the use of cars because they are polluting, they usurp fossil fuels, or are dangerous. Indeed, it is the harm to users or non-users caused by the technology that makes the pressure exerted undesirable. Regarding lifelogs, a situation may be created in which one has to choose between the use of a technology that negatively affects their privacy, autonomy, and the good, and the negative consequences of refusing to lifelog. The situation before the advent of lifelog technology may have been preferable.

Lifelogs may change society in a myriad of expected and unexpected ways. In a society in which lifelogs are the norm rather than a rarity one might be expected to be able to hand over more information than in a society without lifelogs. Companies may assume their consumers use lifelogs, and/or reward the use of lifelogs by incorporating lifelogs into their organisation and/or functioning. Corporations, such as insurers or financial institutions, may request lifelog data to determine eligibility for certain services because they assume people to have this information readily available. Also, authorities can expect their populace to produce

more data when applying for public services. In the worst case, someone who ignores their lifelog or refuses to use can be considered criminally irresponsible. One may think of scenarios in which parents may be considered negligent when not monitoring the behaviour of their children through lifelog equipment.

This kind of pressure only arises when lifelogs are firmly embedded within society and many have already chosen to lifelog. The fact that many are using a technology does not signify that the technology is ethically desirable. For one, there may be more subtle forms of force at play that can make people lifelog without them necessarily considering lifelogs desirable, e.g. the fact that lifelogs can be positional goods. Also, many can be wrong. People can structurally undervalue the importance of values such as privacy and autonomy and structurally overvalue other values such as happiness and convenience. People can also underestimate the negative consequences of the technology or the technology can prove beneficial to lifeloggers when used by a selected group but less desirable when used by many. The latter can be the case when governments begin demanding structural access to lifelog data because lifelog technology has become a significant data source for surveillance, or when corporations, such as data brokers or insurance companies, start using lifelog data for risk profiles or quotes. Finally, the technology can change for the worse while high lock-in costs can make it unattractive to switch, e.g. this can happen when the privacy policy of a lifelog or lifelogging devices is changed and lifeloggers have to choose between losing years of data or accepting the new terms and conditions.[169]

A final concern may be that lifelogs become imposed on consumers as an unavoidable by-product of another service. An example of this is Google, which had a policy of integrating its social network Google+ so its network became a necessary by-product to enjoy some services. In addition to an account for Gmail (email service), YouTube (video-website), and other Google services, one would also be set up with a public Google+ account (Efrati 2013). The advantage of this bundling of services was that Google could generate more revenue because it obtained more information for advertisements. The bundling of services could evidently be problematic for one's privacy, but could also impede on one's choice to become a lifelogger. One may not want to give up a particular service that comes with a lifelog account.

---

[169] A more in-depth discussion of this phenomenon can be found in the chapter on privacy (*5.2.1.5 Creating a Panopticon*).

Conclusion: Embedding lifelogs into the fabric of society does not necessarily bring the condition of being free from controlling influences below an acceptable standard. Technology becoming indispensable to function in daily life is often not considered an argument against it unless the technology unfairly or undesirably curtails one's options. One approach is ensuring that issues with privacy and other ethical principles and values are minimised and opportunities for autonomy and the good are maximised. Another approach is to provide the lifelogger with much control over the content of lifelog data. As the lifelogger could alter content, the data stored within the lifelog become less reliable for third parties. Therefore it becomes less attractive for third parties to integrate lifelog content into their organisation. Finally, companies should never attempt to impose lifelog technology upon their consumers.

7.2.4 Summary

The three conditions for autonomous decision-making discussed can all three be compromised when offering lifelog technology.

1) The disclosure of information can be dissatisfactory as lifeloggers are dependent on the discretion of companies offering lifelog technology. This issue can be adequately addressed by offering comprehensive and understandable information to lifelogger beforehand.

2) The choice whether to become a lifelogger is complex and people faced with this decision may lack the competence to make an autonomous decision as commercially available lifelog technology can reach a great variety of people. By designing the lifelog so that complexity is reduced, developers can reduce the minimum level of competence needed for the decision to become a lifelogger. The lifelog company can also decide to vary functionality according to competence usually assigned to people within particular age brackets. Some features might not be made available to minors as they are often considered to lack the competence to deal with the complexity of the choice.

3) There may be different kinds of pressure exerted on consumers to become lifeloggers. Potential pressure caused by government agencies on citizens to show their innocence seems either insignificant or not caused by lifelog technology and therefore irrelevant. Social pressure is more disconcerting. Being forced by members of one's close environment to lifelog so that they can check one's behaviour can greatly reduce one's

autonomy. However this kind of pressure does not seem to occur often. Societal pressure can be more subtle as people can be blamed for not using lifelogs. There is no obvious way to address this issue but the issue seems hardly decisive. Two other issues are the embedding of lifelogs within society and lifelogs being positional goods. Often these kinds of pressure are accepted unless the status quo before the advent of lifelogs was preferable. By reducing the information stored by lifelogs about other people and ensuring that lifelogs are altogether beneficial, the issues with societal pressure to lifelog can be somewhat alleviated or accounted for. More so, lifelog companies can give lifeloggers extensive control over the content produced allowing lifeloggers to manipulate data thereby making the data less reliable and useful to organisations or others.

That some people will lifelog without having had an autonomous choice is unavoidable. It is impossible for a lifelog company to ensure beyond doubt that all their consumers are competent, have sufficient personal freedom, or, in fact, are sufficiently informed. Nonetheless, if one would require autonomous decisions without exception innovation would be too stringently curtailed. In addition, prospective lifeloggers could autonomously choose to forfeit their decision, e.g. people could decide to reject the information offered to them or allow other people to choose for them. However, the developers can take measures so that an autonomous choice is not precluded or unlikely.

7.3   Recommendations

There are five general things to say about the recommendations (*Cf.* Jacquemard 2014):

1) One evident concern is transparency. Companies offering lifelog services should disclose the relevant information necessary to make an informed choice in a way that is comprehensible for the prospective lifelogger without her having to spend much time and resources to understand the information presented to her.

2) Even though it seems impossible to establish the competency of a prospective lifelogger on an individual basis, it must be possible to determine some standards of competency for particular groups and adjust functionality and information accordingly. Age has already been mentioned as a coarse indicator for competency. Children within particular age brackets might lack the competence to make intricate decisions regarding their privacy and that of others. Information can be presented to suit the competency levels usually assigned to young children. The elderly might not be accustomed to the novelty of

technology (and the vocabulary associated with it) and fail to properly grasp its possibilities. One way to deal with this is to adjust the information presented and the form in which it is presented to the competency levels of different groups. Another way to deal with this issue is by making the choice to become a lifelogger less complicated. By avoiding moral, social, and legal problems and improving user-friendliness one can lower the level of competence required for an autonomous decision about becoming a lifelogger. Decreasing the likelihood and severity of moral, social, and legal problems also means that prospective lifeloggers do not have to make complicated decisions about privacy and the importance of personal information.[170]

3) Regarding the freedom from controlling influences, the recommendations are based on the idea that by extending the lifelogger's control over the content of lifelog data the reliability of data is undermined; data become less trustworthy as a source of information and therefore also less functional to be used by organisations as an integral part of their functioning. As the data will not be requested by organisations there will be lesser pressure extended upon consumers to lifelog. One can undermine the reliability in a constructive way by providing lifeloggers and people being lifelogged, as far as possible, with control over the whole process of lifelogging and the data contained within a lifelog. Recommendations offered in the chapter on privacy are aimed to increase control (*4.6 Recommendations*).

4) Extending control will not take away all pressure on a prospective lifelogger to start lifelogging. There may still be a need to safeguard reciprocity when lifelogs capture personal information about others and they can still be positional goods. Minimising or avoiding the capturing of information about others is a manner to avoid some issues with the need to maintain reciprocity. Adherence to the recommendations provided in the chapter on privacy might also prove beneficial for this issue also because these recommendations aim to provide the lifelogger with greater control over the content of a lifelog (*4.6 Recommendations*).

---

[170] The proposed actions of assessing competency levels regarding a particular technology and addressing the technology to suit these competency levels shows similarities with the 'goodness-of-fit ethic as introduced by Fisher (2003). She states that informed consent during research involving adults with mental retardation and development disabilities requires "(a) an examination of those aspects of the consent setting that are creating or exacerbating consent vulnerability and (b) consideration of how the setting can be modified to produce a consent process that best reflects and protects the consumer's hopes, values, concerns, and welfare" (Fisher 2003, 29).

5) Some of these issues are caused because lifelogs are, on balance, detrimental to the privacy, autonomy, and the good of the lifelogger. A widespread use of lifelogs would create a dilemma because one either has to choose between the negative effects of using lifelogs or the negative effects caused by not having access to lifelogs. These issues can be avoided by designing the technology bearing ethical principles and values in mind so that lifelogs will in sum be beneficial. Again, recommendations made regarding privacy, autonomy, and the good are of utmost importance.

The recommendations below may not eradicate all concerns associated with the autonomous character of becoming a lifelogger. However, they might bring these concerns to an acceptable level.

1. Disclosure about functioning of the device: Prospective lifeloggers should be provided with sufficient and comprehensible information by the developers. The consumers require information about the functioning of the lifelog and the purposes for which lifelogs are to be used.

2. Age restrictions: Developers can opt to set age restriction for particular features of the lifelog or set a minimum age below which one is not allowed to lifelog. A minimum age might be desirable as the usage of lifelogs might be too complex for children of a certain age. However, it may be possible to diminish risk regarding privacy, autonomy and other principles so that even young children (and maybe their parents) could benefit from the use.[171]

3. Address concerns regarding privacy: By respecting privacy one avoids some moral issues arising from lifelogs as well as allows the lifelogger to exert more control over content of lifelogs. Recommendations to alleviate privacy concern are provided above (*4.6 Recommendations*).

4. Address concerns regarding autonomy: By respecting autonomy one avoids some moral issues arising from lifelogs. Recommendations to alleviate autonomy concerns are provided above (*5.4 Recommendations*). In addition, autonomy requires disclosure. Lifelogs should inform prospective lifeloggers about their features and functionalities.

---

[171] Parents may profit from information about their health or diet.

5. <u>Address concerns regarding beneficence:</u> By respecting concerns about beneficence one avoids some moral issues arising from lifelogs and the possible harms, which might make the decision to become a lifelogger less complex. Recommendations to alleviate concern with beneficence are provided in the previous chapter (*6.3 Recommendations*).

6. <u>Inform about harms to autonomy, privacy, and the good</u>: The potential lifeloggers should be informed about the potential benefits and risks to privacy, autonomy, and the good associated with the use of the technology, because these might be relevant when faced with the choice to begin lifelogging. A lifelog company should aim to identify the potential harms expected from lifelog technology.

7. <u>Adjust functionality to suit competency:</u> For example, the use of wearable cameras for young children exposes them to dilemmas regarding privacy and may leave them vulnerable when intimate photos of themselves or others surface. While wearable cameras seem undesirable pedometers measuring activity can be useful and little harmful. In addition, in order to benefit from lifelog technology, the user needs to have the competence to put the information into the right context and assess and appreciate its limited usefulness.

8. <u>Allow lifelogger to choose:</u> The company offering lifelog services should not impose the use of lifelog technology on its users. Aggressive marketing, for example by making lifelogs an unavoidable by-product of other services, should be avoided.

9. <u>Appropriateness of information feedback:</u> Information feedback should be provided in an appropriate form. The information obtained from a lifelog can be fed back to lifeloggers in various forms. The functionality of lifelogs should be adjustable to the competence of the lifeloggers. Children, for example, are a vulnerable population. If the use of lifelogs by children cannot legally be regulated or practically prevented, the content and the way it is presented can be adjusted for them. One could think of the use of metadata with various levels of abstraction using negative descriptions as 'no alcohol consumed', or, 'maintaining a healthy lifestyle', or positive descriptions such as 'at school', or, 'within proximity of the house' instead of raw photos, GPS coordinates or other data.

10. <u>Identify and inform vulnerable groups:</u> Some groups of people may be less competent to decide on whether or not to use a lifelog, such as persons suffering from bipolar and

unipolar depression. The lifelog company should aim to identify the risks associated with these particular groups and disclose these risks to prospective users.

7.4 Conclusion

Three conditions for autonomous decision-making have been examined; namely, disclosure, competence, and being free. The extent to which these conditions are fulfilled can vary. As a consequence becoming a lifelogger can be lesser or more autonomous depending on the design and use of lifelogging applications and devices and the environment in which they are situated.

The information provided by the companies offering lifelog technology can be lacking. In order to have sufficient understanding about the functioning of the device, developers need to provide detailed information. The outside of lifelog technology will often reveal little about its functioning. In the situation that the developer fails to properly inform potential lifeloggers about the devices, the ability of these prospective users to make decisions according to their own values and desires will be impaired. Also, lifelogs will be potentially available to a wide variety of people who may lack the competence to make informed decisions about the usage of the technology. Even the condition of being free can be compromised as there might be various forms of pressure exerted on prospective lifeloggers to become a lifelogger.

Much will depend on the design of the lifelog. The condition of disclosure can be optimised by companies providing people with relevant information in a suitable form. The difference in competence levels is likely to require developers to limit their target market by excluding some categories of potential lifeloggers (for example by setting minimum ages) from the technology or some of its features. Another way to address issues with competency is by avoiding ethical, moral, or legal problems stemming from lifelogs. These problems make the decision to become a lifelogger less complicated. The condition of being free is more difficult to improve, but strategies to constructively undermine the reliability of lifelogs by maximising control of the lifelogger over the content stored with the lifelog is one way to address this issue. Another way to address this issue is to minimise or avoid capturing information about others.

This chapter was concluded with recommendations to address issues with becoming a lifelogger. The checklist that can be found in the appendix (*Appendix D: Checklist for*

becoming a lifelogger) can be used to identify these issues while the recommendation are ways in which these issues can be addressed.

Bibliography

Ackerman, S. 2013. NSA warned to rein in surveillance as agency reveals even greater scope [Online]. *The Guardian.* Available from: http://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing [Accessed 02-11-2013].

Allen, A.L. 2007. Dredging up the past: Lifelogging, Memory, and Surveillance. *The University of Chicago Law Review*, 75(1), pp. 47-74. Berlin I. Four essays on liberty. Oxford: Oxford University Press, 1969.

Ball, J., Borger, J., & Greenwald, G. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security [Online]. *The Guardian.* Available from: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed 16-10-2013].

Bazelon, E. 2011. Why Facebook Is After Your Kids [Online]. *The New York Times*. Available from: http://www.nytimes.com/2011/10/16/magazine/why-facebook-is-after-your-kids.html [Accessed 21-01-2014].

Beauchamp, T.L. & Childress, J.F. 2009. *Principles of Biomedical Ethics: Sixth Edition*. New York & Oxford: Oxford University Press.

Bostrom. N. & Roache, R. 2008. Ethical Issues in Human Enhancement. *IN:* Ryberg, J., Petersen, T. & Wolf, C. (Eds.) *New Waves in Applied Ethics*. New York: Palgrave MacMillan, pp. 120-152.

Boyd, D., Hargittai, E., Schultz, J. & Palfrey, J. 2011. Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday,* 16(11).

Brandom, R. 2014. Microsoft offers overseas data storage in response to NSA concerns [Online]. *The Verge.* Available from: http://www.theverge.com/2014/1/22/5335434/microsoft-offers-overseas-data-storage-in-response-to-nsa-concerns [Accessed 23-01-2014].

Castro, D. 2013. *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* Washington, DC: Information Technology and Innovation Foundation

Charland, L. 2011. Decision-Making Capacity. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy. Summer 2011*. Available from: http://plato.stanford.edu/entries/decision-capacity/ [Accessed 21-01-2014].

Cheng, J. 2012. Three years later, deleting your photos on Facebook now actually works [Online]. Available from: http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/ [Accessed 23-01-2014].

Children's Online Privacy Protection Act of 1998, 5 U.S.C. 6501–6505 [Online]. Available from: http://www.coppa.org/coppa.htm [Accessed 21-01-2014].

Commission for Communications Regulation. 2005. *Irish Communication Market: Quarterly Key Data Report September 2005* [Online]. Available from: http://www.comreg.ie/_fileupload/publications/ComReg0573.pdf [Accessed 03-06-2014].

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

Economist. 2011. Digital revolution [Online]. *The Economist.* Available from: http://www.economist.com/node/18529875 [Accessed 17-09-2013].

Efrati, A. 2013. There's No Avoiding Google+ [Online]. *The Wall Street Journal.* Available from: http://online.wsj.com/news/articles/SB10001424127887324731304578193781852024980 [Accessed 11-06-2014].

Eyal, N. 2011. Informed Consent. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy. Fall 2012*. Available from: http://plato.stanford.edu/entries/informed-consent/ [Accessed 20-01-2014].

Federal Trade Commission. 2013. *Federal Trade Commission 2013* [Online]. Available from: http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#genquestions [Accessed 24-01-2014].

Felten, H. & Pierik, C. 2011. *Preventie suïcidaal gedrag allochtone meiden: Kennis in kaart*. Utrecht: Movisie.

Fisher, C.B. 2003. Goodness-of-fit ethic for informed consent to research involving adults with mental retardation and developmental disabilities. *Mental Retardation and Developmental Disabilities Research Reviews*, 9(1), pp. 27-31.

Gartner. 2013. *Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time*. Available from: http://www.gartner.com/newsroom/id/2573415 [Accessed 01-05-2014].

Gellman, B. & Soltani, A. 2014. NSA surveillance program reaches 'into the past' to retrieve, replay phone calls [Online]. *The Washington Post*. Available from: http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html [Accessed 24-04-2014].

Gellman, B., Tate, J., & Soltani, A. 2014. In NSA Intercepted Data, Those not Targeted Far Outnumber Foreigners who are [Online]. *The Washington Post*. Available from: http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [Accessed 09-09-2014].

Glanz, J., Larson, J., & Lehren, A.W. 2004. Spy Agencies Scour Phone Apps for Personal Data [Online]. *The New York Times.* Available from:

http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?hp&_r=1 [Accessed 27-01-2014].

Gray, S. The inquiry that put Ahern finances in spotlight. *The Guardian.* Available from: http://www.theguardian.com/world/2008/apr/02/ireland4 [Accessed 12-09-2013].

Greenwald, G. 2013. NSA collecting phone records of millions of Verizon customers daily [Online]. *The Guardian*. Available from: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Accessed 24-04-2014].

Informa. 2013. Africa Telecoms Outlook 2014. Available from: http://files.informatandm.com/uploads/2013/11/Africa_Telecoms_Outlook_Low_resolution.pdf [Accessed 01-05-2014].

IT News Africa. 2013. Smartphone shipments to Africa up 21.5%. Available from: http://www.itnewsafrica.com/2013/09/smartphone-shipments-to-africa-up-21-5/ [Accessed 01-05-2014].

Jacquemard, T., Novitzky, R., O'Brolcháin, F., Smeaton, A.F. & Gordijn, B. 2014. Challenges and opportunities of lifelog technologies: a literature review and critical analysis. *Science and Engineering Ethics*, 20(2), pp. 379-409.

Mansfield, I. 2013. Explosive Smartphone Growth, Cannibalises Indian Feature Phone Sales. *Cellular News*. Available from: http://www.cellular-news.com/story/63271.php [Accessed 01-05-2014].

Mill, J.S. 1859. *On Liberty*. London: Penguin.

O'Hara, K., Tuffield, M. & Shadbolt, N. 2009. Lifelogging: Privacy and Empowerment with Memories for Life. *Identity in the Information Society*, 1(2), pp. 2-3.

Schofield, J. 2004. How to save your life [Online]. *The Guardian*. Available from: http://www.theguardian.com/technology/2004/aug/19/onlinesupplement.blogging [Accessed 22-01-2014].

Schurgin O'Keeffe, S. & Clarke-Pearson, K. 2011. The Impact of Social Media on Children, Adolescents, and Familie. *PEDIATRICS,* 127(4), pp. 800-804.

Staten, J. 2013. The Cost of PRISM Will Be Larger Than ITIF Projects [Online]. *Forrester*. Available from: http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

Talbot, D. 2014. Android App Warns When You're Being Watched [Online]. *MIT Technology Review*. Available from: http://www.technologyreview.com/news/523981/android-app-warns-when-youre-being-watched/ [Accessed 14-03-2014].

TED. 2011. *Hasan Elahi: FBI, here I am!* [Online]. Available from: http://www.ted.com/talks/hasan_elahi.html [Accessed 23-05-2012].

Wyatt, E. & Miller, C.C. 2013. Tech Giants Issue Call for Limits on Government Surveillance of Users [Online]. *The New York Times.* Available from: http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html?smid=tw-nytimestech&seid=auto&_r=0 [Accessed 23-01-2014].

8 Conclusion

Introduction

The aim of this study was to contribute to a responsible development of lifelog technology. In this conclusion a short summary of the results is provided and an outlook offering suggestions for further research on a responsible development of lifelog technology will conclude this chapter.

8.1 Summary of the results

The inquiry commenced with a short discussion on the definition and characteristics of lifelog technology. In addition, a literature review has been undertaken to identify existing ethical challenges and opportunities in the current scholarly debate on the ethics of lifelog technology. The review revealed a rich debate that nonetheless left challenges and opportunities untouched or insufficiently elaborated upon. Against this backdrop, ethical challenges and opportunities were identified. Four keys sets of ethical challenges and opportunities have been identified. The first three discussed the consequences of the usage of lifelog technology for lifeloggers and non-lifelogger for their (1) privacy, (2) autonomy, and (3) good. The fourth discussed autonomy-related concerns regarding the conditions under which one becomes a lifelogger. The identification and discussion of these moral challenges and opportunities formed the foundation for the formulation of design recommendations that should be implemented to develop lifelog technology conscientiously with due care for ethical obligations.

8.1.1 Regarding privacy

The privacy of both lifeloggers as well as non-lifeloggers can be compromised by the use of lifelog technology. The discussion of privacy and lifelogging showed only one minor ethical opportunity related to privacy and exposed several major ethical challenges. A responsible development of lifelog technology is expected to reduce the problems with privacy significantly, but cannot categorically exclude all risks to privacy. Thus, argued solely from the principle of respect for privacy, further development of lifelog technology seems ethically undesirable: there need to be other principles at play that weigh more forcefully in favour of lifelog technology to render the development desirable.

Finally, a set of recommendations has been provided that can be used to address issues caused by lifelog technology with privacy. These recommendations are aimed primarily to increase control over personal information for both the lifeloggers and non-lifeloggers. In an attempt to reduce the time and resources needed to identify challenges relating to privacy, a checklist has been advanced in the appendices (*Appendix A: Checklist for privacy*).

8.1.2 Regarding autonomy when being a lifelogger

The second key set of challenges and opportunities was related to the impact of the use of lifelog technology on the autonomy of lifeloggers and non-lifelogger. The ethical challenges and opportunities were considered on the levels of deliberation and execution. The analysis demonstrated that usage of lifelog technology could – depending on its design and contextual variables - both promote as well as hinder the deliberative and executive autonomy of both lifeloggers and non-lifeloggers. As a result, the principle of respect for autonomy can generate *prima facie* obligations demanding a halt to or favouring the further development of lifelog technology, depending on the circumstances and design.

In order to address challenges and opportunities regarding autonomy, recommendations were offered. These recommendations were primarily concerned with reaching a high standard for the quality of information and the need for lifelog technology to conform to demands made to protect privacy. Similar to the chapter on privacy, a checklist was offered in the appendices (*Appendix B: Checklist for autonomy*) to obtain a swift insight into ethical challenges and opportunities regarding this set of autonomy-related concerns.

8.1.3 Regarding beneficence

The third key set of challenges and opportunities related to beneficence. In this study, the effect of lifelog technology on ten aspects of the good has been discussed. The analysis demonstrated that lifelog technology can have significant benefits and detrimental effects on the good experienced by lifelogger and non-lifeloggers. Accordingly, *prima facie* duties of beneficence can both favour and disfavour a further development of lifelog technology depending on the design of the technology.

There are also recommendations provided to optimise the balance of good over evil. The recommendations made for autonomy and privacy are also relevant to beneficence-related concerns, as a failure to protect privacy and autonomy also negatively affects the good

of lifeloggers and non-lifeloggers. Again, a checklist was advanced to identify issues with beneficence (*Appendix C: Checklist for beneficence*).

8.1.4 Regarding autonomy when becoming a lifelogger

The fourth key set of issues revolved around becoming a lifelogger. The conditions under which one becomes a lifelogger may preclude the lifelogger-to-be from making an autonomous decision about the use of the technology. In case the decision of the lifelogger is autonomous, one could argue that he considered lifelogging in his best interests despite the potential negative effects. After considerable thought, it was deemed that there were no opportunities and solely challenges identified with regard to this topic of concern.

Recommendations were suggested to tackle the challenges associated with becoming a lifelogger. These recommendations were aimed at optimising disclosure and the minimisation of complexity of the choice to lifelog. Similar to the three previous chapters, a checklist has been provided as an appendix (*Appendix D: Checklist for becoming a lifelogger*).

8.2 Outlook

This study is concluded with five suggestions for future research.

8.2.1 Other principles

One limitation of the study at hand is that there may be other relevant principles at play. The list of principles applied here is not exhaustive. This limitation is inherent to the methodology as applied here. Ross acknowledged that his list of *prima facie* duties was open-ended as he stated: "[o]f *prima facie* duties I suggest, without claiming completeness or finality for it, the following division" (Ross 2002, 20). Further on he held that "[i]f the objection is made, that this catalogue of the main types of duty is an unsystematic one resting on no logical principle, it may be replied, first, that it makes no claim to being ultimate" (Ross 2002, 23).

Therefore, there might be other principles relevant to be considered when thinking about the ethics of lifelog technology. An important example largely missing in the current study is the principle of justice. It is a complex principle with many interpretations and implications. Generally justice concerns equitable and appropriate treatment in light of what people are entitled to. Issues with justice in conjunction with lifelog technology have been alluded to throughout this study. In the chapter on autonomy it was discussed that particularly minorities could suffer most from a failure to protect privacy (*5.3.1.1 Diminishments by*

governmental agencies). Another example of an issue with justice, to be found in the chapter on autonomy, was that biased lifelog content could favour particular cultural conceptions (*5.2.1.1 Biases*). In the chapter on beneficence, the concern was mentioned that the facilitation of a covert processing of personal data could allow discriminatory beliefs and values to flourish (*6.2.7 Affiliation*). In the chapter on becoming a lifelogger an issue was identified with lifelog technology being imposed on the vulnerable whose freedom could be further imposed with the introduction of lifelog technology (*7.2.3.2 Social pressure*).

Hence, respect for justice may provide relevant moral duties to developers and a discussion on the principle of justice could elucidate these duties. Indeed, it might have implications when optimising the conditions for a responsible design of lifelog technology, as sometimes one may prefer a just spread of harm and benefits above more benefits.

8.2.2 Other stages of inquiry

This dissertation concentrated upon issues with lifelog technology that manifest when it is available as an end-product for members of the general public for private purposes when using lifelogs or becoming a lifelogger.

The moral challenges and opportunities that arise when a lifelogger stops using lifelog technology have not been discussed. The prediction is that the main set of challenges and opportunities within this domain relate to privacy and, more specifically, with control over personal information that remains in the possession of the lifelog company.

Ethical issues can also manifest themselves during the stage of research and development and the stage of trials with human participants. In the literature review, the stage of research and development was identified as a stage that has yet to be addressed in the academic debate on the ethics of lifelog technology. Issues do occur during this stage. For example, design could lead to patent infringements suits. The lawsuits between Apple and Samsung showed the quandaries that can result from perceived patent infringements (Apple, Inc. v. Samsung Elecs. Co., Ltd. 2013a & 2013b). The trial stage is another interesting field for an ethical inquiry. A few sources had mentioned potential issues at the trial stage (3.2.1.8 Issues concerning the protection of research subjects), but only one of them has an elaborate ethical framework, although one that is highly specialised, namely applied to research in health behaviour with the SenseCam (Kelly et al. 2013). Trials with human research participants provoke ethical issues, such as data ownership, privacy of the research

participants, and privacy of lifelogged third parties that were not participating in the trials, which could be minors. In addition, prominent researchers in the field, such as Mann (2002), Gurrin (The Economist 2013), and Bell (Bell & Gemmell 2009), are also famously auto-experimenters. The ethical challenges and opportunities associated with trials with auto-experimenters might differ from those with human participants, who are not involved in the design of the technology. Shilton (2010), for example considers self-experiments to be advantageous for the ethical development of technology as they provoke discussions about ethics within the design team. This might also be the case for lifelog technology.

8.2.3 Other usages of lifelogs

This study focused on the use of lifelogs by private citizens for private purposes. However, as has been shown in the discussion on the characteristic of the technology (*2.3.2 Purposes* and *2.3.3 Users*), lifelog technologies can be deployed in many other settings than the scenario, which has been the backdrop to identify challenges and opportunities in this study. Lifelogs that are enforced by employees or prescribed by medical professionals give rise to different ethical issues.

One such scenario would be the use of lifelogs for persons with dementia (PwDs) suffering from short-term memory loss. In this scenario, lifelogs might be used to address a need that is typically not as urgent for people, who do not suffer from memory impairments, namely to provide cues about the recent past. The issues with privacy would be of a different magnitude partly because the potential target group - PwDs in a particular phase of their human condition - has become smaller. In addition, challenges associated with privacy are expected to be slightly different, e.g. PwDs are unlikely to use modern communication channels, such as social networking sites as Facebook or Twitter, to share their data on the Internet. Moreover, their memory impairment may also negatively affect their capacity for autonomous choice, which also changes the set of challenges and opportunities invoked related to autonomy. Indeed, the fact that lifelogs might be able to retrieve information about their past that PwDs would not have had without lifelog devices, could provide them with a sense of empowerment that persons without dementia would not experience from the technology. In summary, the interests and the competence commonly associated with this group, changes the set of ethical challenges and opportunities invoked by lifelog technology.

Such possible scenarios and specific applications of lifelog technology are too manifold to be discussed comprehensively, but separate studies can be useful.

8.2.4 Conflicting recommendations

The balancing of conflicting recommendations is another area that requires further research. Conflicts are largely expected between recommendations to protect privacy and recommendations to realise opportunities related to the good and autonomy. The former set of recommendations requires reticence in creating and digitally storing personal information, while the latter may require the creation of personal data and the deployment of recording technology. For example, there is considerable latitude when applying the recommendation that information about others should be minimised. For sousveillance, one needs to deploy a recording device that captures information about others indiscriminate of authority. It is therefore probable that the devices suitable for sousveillance reduce privacy considerably. However, one could consider sousveillance to be an advantage to autonomy that outweighs concerns for privacy. For instance, the need for recording devices may be more urgent in an environment in which the chances are high that one encounters corrupt officials or fellow citizens with potential detrimental consequences.

Unfortunately, it is unattainable to provide definite solutions when such conflicts occur. The specific circumstances of a given situation in which lifelog technology is deployed largely determine the weight of the *prima facie* ethical duties. In addition, there is a broad spectrum of variety possible regarding the functioning and design of lifelog applications and devices: for example, an application quantifying email behaviour invokes a different set of challenges and opportunities than wearable cameras. This wide spectrum of contingencies precludes the predetermination of outcomes in case of conflicting principles.

8.2.5 Recommendations for other stakeholders

The purpose of this study was that its findings could contribute to an ethical responsible development.[172] The recommendations that concluded each chapter were aimed at the design of lifelog technology. There are, however, other stakeholders involved that shape the development and application of lifelog technology and the environment in which lifelogs function for which recommendations could be formulated, such as consumers and regulators,

---

[172] Approaches that aim to guide an ethically responsible development of technology have been suggested by, amongst others, Friedman (1996) as 'value sensitive design' and by Flanagan, Howe, and Nissenbaum (2008) as 'values at play'. Whereas, traditionally ethics is a field that evaluates past events, to incorporate ethics into design, the field of ethics need to be future orientated. Van den Hoven referred to this as the "frontloading of ethics" (Van den Hoven 2005). There are several scholars that have argued that such an approach is succesfull (Fisher 2007; McGregor & Wetmore 2009; Shilton 2010). Manders-Huits and Zimmer (2009) and Shilton (2013) provide some pragmatic measures that can be taken to make such an approach successful.

which have other instruments than design to address ethical challenges and opportunities. The impact of consumers or regulators has been alluded to throughout this study, e.g. mentions of the importance of social norms (*4.4.2 Existing moral, social and legal norms*) and government agencies obtaining and using personal information (*4.2.2.1 Reduced control over personal information*).

This study showed that the design of lifelog technology can have negative implications for the privacy, autonomy, and the good of its users. It is extremely unlikely that regulations alone, without any effort from the developers to meet ethical obligations, would be sufficient to ensure an ethical responsible design. In addition, although regulation is important, it could be inappropriate to address many challenges identified above. For instance, in the chapter on autonomy, a recommendation was provided that one needs to be sensitive towards bias (*5.4 Recommendations*). The prevention of undesirable biases advocated here was not exclusively aimed at commonly accepted limitations to freedom of speech, such as slander or hate speech, which can be regulated for, but at more subtle forms of self-determination. An authority deciding which values and beliefs are acceptable to be promoted seems to be an undesirable restriction of the freedom of expression in itself.

The choice to provide recommendations for designers rather than for consumers or regulators can also be explained by the chronology of development: at this stage there is still much uncertainty about the shape and form of lifelog technology and, consequently, how lifelog technology *can* be used or regulated while alterations of the technology at this stage are easier to accomplish than when the technology is nearly finished or already widely available. Furthermore, negative results from unsound technology might drive away investors and consumers: addressing design at an early stage of development prevents investments into avenues that lack societal support and protects consumers from harm. Therefore, it is also important to the field of technology that ethical issues are addressed early in the development stage.

Bibliography

*Apple, Inc. v. Samsung Elecs. Co., Ltd.,*Case No. 2012-1507 (Fed. Cir. Jan. 31, 2013).

Apple, Inc. v. Samsung Elecs. Co., Ltd., Case No. 2013-1129, 2013 WL 444755 (Fed. Cir. Feb. 4, 2013).

Bell, G & Gemmell, J. 2009. *Total Recall: How The E-Memory Revolution Will Change Anything*. New York: Dutton.

The Economist. 2013. A search engine for the self [Podcast]. Available from http://www.economist.com/blogs/babbage/2013/11/cathal-gurrin-life-logger# [Accessed 27-03-2014].

Fisher, E. 2007. Ethnographic Invention: Probing the Capacity of Laboratory Decisions. *NanoEthics*, 1(2), pp. 155-165.

Flanagan, M., Howe, D.C., & Nissenbaum, H. 2008. Embodying Values in Technology: Theory and Practice. *IN:* Van den Hoven, J. & Weckert, J. (eds.) *Information technology and moral philosophy*. Cambridge: Cambridge University Press, pp. 301-321.

Friedman, B. 1996. Value-Sensitive Design. Magazine interactions, 3(6), pp. 16-23.

Hoven, M.J. Van Den. 2005. Design for Values and Values for Design. *Information Age +, Journal of the Australian Computer Society*, 7(2), pp. 4-7.

Kelly, P., Marshall, S.J., Badland, H., Kerr, J., Oliver, M., Doherty, A.R. & Foster C. 2013. An Ethical Framework for Automated, Wearable Cameras in Health Behavior Research. *Am J Prev Med*, 44(3), pp. 314-319.

Manders-Huits, N. & Zimmer, M. 2009. Values and Pragmatic Action: The Challenges of Introducing Ethical Intelligence in Technical Design Communities. *International Review of Information Ethics*, 10(2), pp. 37-44.

Mann, S. 2002. Sousveillance [Online]. *Wearcam.org.* Available from: http://wearcam.org/sousveillance.htm. [Accessed 05-04-2012].

McGregor, J. & Wetmore, J.M. 2009. Researching and Teaching the Ethics and Social Implications of Emerging Technologies in the Laboratory. *NanoEthics*, 1(2), pp. 17-30.

Ross, W.D. 2002. *The Right and the Good*. New York: Oxford University Press.

Shilton, K. 2010. Technology Development with an Agenda: Interventions to Emphasize Values in Design. *IN: Proceedings of the 73rd Annual Meeting of the American Society for Information Science & Technology (ASIST). Vol. 47. Pittsburgh, PA, October*.

Shilton, K. 2013. Values Levers: Building Ethics into Design. *Science, Technology & Human Values*, 38(3), pp. 374-397.

Appendix A: Checklist for privacy

To simplify the identification of challenges regarding privacy, a checklist is suggested. All items on the checklist and following checklists are formulated as closed questions to which one can reply 'yes', 'no', or 'uncertain'. An answer in the right column indicates a potential challenge for the privacy of lifeloggers or non-lifeloggers.

To clarify some of the terminology, the term 'others' refers to those people who are not the lifelogger (other people than the lifelogger) captured through lifelogging technology.

Table 5: Checklist for privacy

	No challenge or challenge minimised	*Potential challenge*
1. Recording of others		
a. Does the device capture data that refer or can be attributed to others?	*No (go to 3)*	*Yes/Uncertain*
b. Can the lifelogger retrieve information that refers or can be attributed to others by him/her?	*No*	*Yes/Uncertain*
c. Are the data that refer or can be attributed to others minimised?	*Yes*	*Uncertain/No*
d. Is information that can be retrieved by the lifelogger and refers or can be attributed to others minimised?	*Yes*	*Uncertain/No*
e. Do others have the ability to correct their personal data?	*Yes*	*Uncertain/No*
f. Do others have the ability to remove their personal information?	*Yes*	*Uncertain/No*
g. Can the lifelogger share lifelog data?	*No*	*Yes/Uncertain*
h. Is it immediately clear to others when the device/application is actively capturing their personal information?	*Yes (go to 2)*	*Uncertain/No*

i.	Is the lifelog device recognisable as such to others?	*Yes*	*Uncertain/No*
j.	Is it clear to others when the device is active as a lifelogging device?	*Yes*	*Uncertain/No*

2. Lifelogger control over data sources

a.	Is it immediately clear to the lifelogger when the device/application is active?	*Yes*	*Uncertain/No*
b.	Is it possible to stop recording/lifelogging without much ado?	*Yes*	*Uncertain/No*
c.	Does the lifelogger have the option to select the data sources that are used to lifelog?	*Yes*	*Uncertain/No*
d.	Does the lifelogger have the option to permanently remove data (also from back-ups in the possession of lifelog companies)?	*Yes*	*Uncertain/No*
e.	Does the lifelogger have the option to correct or change information within the lifelog (and do these alterations reach back-ups in the possession of lifelog companies)?	*Yes*	*Uncertain/No*
f.	Does the lifelogger have the option to choose the information that can be retrieved from the lifelog?	*Yes*	*Uncertain/No*
g.	Is the lifelogger offered a comprehensible and comprehensive privacy policy?	*Yes*	*Uncertain/No*
h.	Are lifeloggers free to refuse changes in the privacy policy without having to suffer a loss of functionality?	*Yes*	*Uncertain/No*
i.	Are the settings provided to protect the privacy of the lifelogger understandable, known and straightforward to operate?	*Yes*	*Uncertain/No*
j.	Are the purposes for which lifelogs can be used, limited, sufficiently clarified, and acceptable?	*Yes*	*Uncertain/No*

k.	Can the use of lifelog content in any way harm the lifelogger?	*No*	*Yes/Uncertain*
l.	Are there any risks to confidentiality and security?	*No (go to 3)*	*Yes/Uncertain*
m.	Is the lifelog secured to the greatest extent possible?	*Yes*	*Uncertain/No*
n.	Is there any legal clarity about the ownership of data?	*Yes*	*Uncertain/No*
o.	Does the lifelog company possess personal information about the lifelogger that can be subpoenaed?	*Yes*	*Uncertain/No*
p.	Is the lifelogger informed of any potential legal limitations on confidentiality?	*Yes*	*Uncertain/No*
q.	Is the lifelogger the only party that has access to or can distribute personal data?	*Yes*	*Uncertain/No*
r.	Does the lifelog company (or any other company) possess as little personal data from the lifelogger as possible for the lifelog company to function?	*Yes*	*Uncertain/No*
s.	Does the lifelog company refrain from selling or distributing personal data?	*Yes*	*Uncertain/No*
t.	Is the lifelogger sufficiently informed of data in possession of others?	*Yes*	*Uncertain/No*
u.	Does the lifelog allow for third party applications that can access and distribute personal data?	*No*	*Yes/Uncertain*

Appendix B: Checklist for autonomy

The checklist for autonomy is more complex than the one for privacy as lifelogs can also advance autonomy. The number of columns has been increased by one to accommodate the fact that autonomy can also be promoted. (1) The left column contains answers that indicate that either there are no challenges expected or that the challenge has been minimised. (2) The middle column contains answers that indicate there are possible opportunities expected. (3) The right column indicates that there is a potential challenge expected that requires attention.

Table 6: Checklist for autonomy

	No challenge or opportunity	*Potential opportunity*	*Potential challenge*
1. Quality of information			
a. Does the technology provide novel information that is expected to increase the lifelogger's understanding of himself and his environment (for example information about aspects discussed in the chapter on beneficence)?	*Uncertain/No*	*Yes*	
b. Does the technology significantly facilitate the retrieval of that information?	*Uncertain/No*	*Yes*	
c. Is there sufficient justification for the information offered by the technology?		*Yes*	*Uncertain/No*
d. Is the accuracy of the information provided by the lifelog of a sufficient standard to avoid misinformation?		*Yes*	*Uncertain/No*
e. Is there sufficient expertise when developing the lifelog to review the quality of information?		*Yes*	*Uncertain/No*
f. Is it clear to the lifelogger which data sources were used?		*Yes*	*Uncertain/No*
g. Are controversial assertions/or opinions avoided or recognisable as such?		*Yes*	*Uncertain/No*
h. Is information presented in a form that is comprehensible for the lifelogger?	*Uncertain/No*	*Yes*	
i. Is the lifelogger made aware of the limitations and shortcomings of the information presented?	*Yes*		*Uncertain/No*
j. Are the assumptions on which feedback to improve behaviour are based, explained to the lifelogger?		*Yes*	*Uncertain/No*
k. Is the lifelogger informed about opposing theories underlying the feedback as to avoid providing undue weight to fringe theories?		*Yes*	*Uncertain/No*
l. Are the regulations about which information is censored for what reason	*Yes*		*Uncertain/No*

explained?			
m. Are there policies or technological solutions in place to correct undesirable biases within the design?		*Yes*	*Uncertain/No*

2. Manipulation and third party interests

a. If the company intends to influence the lifelogger's behaviour e.g. live healthier or buy a product, does the company inform the lifelogger about these intentions?	*Yes*		*Uncertain/No*
b. Is the lifelogger misled or deceived in any way?	*No*		*Yes/Uncertain*
c. Are other parties allowed or able to influence the retrieval of information?	*Yes*		*Uncertain/No*
d. Are other parties allowed or able to influence the content of lifelogs?	*Yes*		*Uncertain/No*
e. Are other parties allowed or able to influence the presentation of lifelog content?	*Yes*		*Uncertain/No*
f. Is the lifelogger informed about commercial interests invested in the technology?	*Yes*		*Uncertain/No*

3. Privacy

a. Are the recommendations for privacy followed (mainly but not exclusively regarding the following elements)?	*Yes (end)*		*Uncertain/No*
i. Does the device capture information that can be attributed to others?	*No*		*Yes/Uncertain*
ii. Can lifelog data be used by second or third parties?	*No*		*Yes/Uncertain*
iii. Is the lifelog technology secured against second or third parties that could manipulate the content/presentation or retrieval of information?	*Yes*		*Uncertain/No*

Appendix C: Checklist for beneficence

There is one important difference between this list and the ones above. The questions are formulated more abstractly because the various aspects to beneficence make them too numerous for one list. In order to answer this checklist one needs to have some understanding of the capabilities.

Table 7: Checklist for beneficence

	No challenge or opportunity	Potential opportunity	Potential challenge
1. Preliminary			
a. Is there sufficient expertise present to evaluate and guide the development of the technology to prevent harm and/or reap the benefits?	*Yes*		*Uncertain/No*
b. Does the application or devices affect the lifelogger's or non-lifeloggers' capabilities?	*If 'No' (end here), if 'Yes' continue*		
2. Capabilities			
a. Does the application/device affect 'life'?	*If 'No' (go to b), if 'Yes' continue to b*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
b. Does the application/device affect 'Bodily Health'?	*If 'No' (go to c), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
c. Does the application/device affect 'Bodily Integrity'?	*If 'No' (go to d), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*

d. Does the application/device affect 'Senses, Imagination, and Thought'?	*If 'No' (go to e), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
e. Does the application/device affect 'Emotions'?	*If 'No' (go to f), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
f. Does the application/device affect 'Practical Reason'?	*If 'No' (go to g), if 'Yes' continue)*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
g. Does the application/device affect 'Affiliation'?	*If 'No' (go to h), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
h. Does the application/device affect 'Other Species'?	*If 'No' (go to i), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
i. Does the application/device affect 'Play'?	*If 'No' (go to j), if 'Yes' continue*		
i. Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii. Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*
j. Does the application/device affect 'Control over one's Environment'?	*If 'No' (go to 3), if 'Yes' continue*		

i.	Is the technology expected to advance (an element of) the capability?	*Uncertain/No*	*Yes*	
ii.	Is the technology expected to hinder (an element of) the capability?		*No*	*Yes/Uncertain*

Appendix D: Checklist for becoming a lifelogger

As there are no advantages perceived, there is no column with opportunities. The right column indicates that there is a potential challenge.

Table 8: Checklist for becoming a lifelogger

		No challenge expected	**Potential challenge**
1. Avoid issues with privacy			
a.	Does the device capture data that refer to or can be attributed to others?	*No (go to e)*	*Yes/Uncertain*
b.	Are others informed by the device/application that their personal data are captured?	*Yes*	*Uncertain/No*
c.	Is the lifelog device recognisable as such to others?	*Yes*	*Uncertain/No*
d.	Is it clear when the device is active as a lifelogging device to others?	*Yes*	*Uncertain/No*
e.	Do lifelogs promote strong advantages towards people not having lifelogs?	*No*	*Yes/Uncertain*
f.	Are the prospective lifeloggers informed beforehand about the risks to confidentiality and security?	*No*	*Yes/Uncertain*
2. Undermining the reliability of lifelog data			
a.	Is the lifelogger able to remove data?	*Yes*	*Uncertain/No*
b.	Is the lifelogger able to correct information within the lifelog?	*Yes*	*Uncertain/No*
c.	Is the lifelogger able to annotate information within the lifelog?	*Yes*	*Uncertain/No*
3. Competence			
a.	Is the lifelog technology suitable for all ages?	*Yes*	*Uncertain/No*
b.	Can the lifelog application be adjusted to suit the competency of the lifelogger?	*Yes*	*Uncertain/No*

c.	Has the use of lifelog technology been restricted for minors or minors below a certain age?	*Yes*	*Uncertain/No*
d.	Has the use of particular functionalities been restricted for minors below a certain age?	*Yes*	*Uncertain/No*
e.	Is the lifelog technology suitable for people with particular mental disorders?	*Yes*	*Uncertain/No*
f.	Are these persons informed about the risks?	*Yes*	*Uncertain/No*
g.	Are there any other groups of people that may lack the competence to deal with the technology?	*Yes*	*Uncertain/No*
h.	Are these persons informed about the risks?	*Yes*	*Uncertain/No*

4. Informed about the functioning of the device

a.	Is the lifelogger offered a comprehensible and comprehensive privacy policy beforehand?	*Yes*	*Uncertain/No*
b.	Are the purposes to which lifelogs can be used limited and sufficiently clarified beforehand?	*Yes*	*Uncertain/No*
c.	Is the lifelogger informed beforehand about the data sources that are used?	*Yes*	*Uncertain/No*
d.	Is the lifelogger informed about the information that can be retrieved?	*Yes*	*Uncertain/No*
e.	Is the prospective lifelogger informed about the functioning of the lifelog device/application?	*Yes*	*Uncertain/No*
f.	Is the prospective lifelogger informed about his control over the functioning of the device?	*Yes*	*Uncertain/No*
g.	Is the lifelogger informed about potential risks to security and confidentiality?	*Yes*	*Uncertain/No*