Turun yliopisto
University of Turku

IMAGES OF THE FUTURE OF PRIVACY

A privacy dynamics framework and a causal layered analysis of ideal types

Master´s Thesis
in Futures Studies

Author(s):
Matti Minkkinen

Supervisors:
Ph.D. Burkhard Auffermann

31.5.2013
Turku

Turun kauppakorkeakoulu • Turku School of Economics

Table of contents

List of figures

List of tables

1 INTRODUCTION

Privacy is clearly one of the pressing issues of the information age. The topic of privacy is featured in newspaper articles literally every day. Surveillance cameras are installed in school toilets (Vasama, 2012), Facebook's privacy policies are regularly discussed (Ahlroth, 2010), banks refuse to hand over customer information that they have gathered (Malmberg, 2012) and the European Commission has recently published a proposal for a new data protection regulation to update and reform the Data Protection Directive from 1995 (European Commission, 2012). Privacy concerns are often connected with new and emerging technologies. Technological systems such as CCTV cameras, radio-frequency identification (RFID) tags and GPS tracking regularly evoke discussion and fears among the public. The potential for surveillance and monitoring seems to constantly increase. At the time of writing, newspapers are discussing the privacy concerns raised by Google Glass, a potentially transformative new technology enabling a camera and a screen to be unobtrusively placed in a pair of eyeglasses (Arthur, 2013). In addition to newspaper coverage, countless books and articles have been written and academic seminars have been held on topics related to privacy and surveillance. In the quickly changing field of privacy concerns raised by technology, it seems that a scholarly account would become obsolete within months of its writing. On the other hand, there are also constant and recurring themes within privacy concerns. Current privacy concerns raise an important question about the future. If this is possible now, what will happen tomorrow?

In this thesis, I will analyse ideal-typical images of the future of privacy held by non-experts. The aim is to examine currently held images of the future and the assumptions behind them. The subjective images of the future are set against the objective background of a conception of privacy as a social phenomenon and the ways in which the level of privacy changes over time through the influence of technologies, actors, interests and practices. The theoretical background is a combination of critical futures studies and critical realism as well as the dialectic of subjective and objective futures, and causal layered analysis is used as the central methodological tool.

I will argue that current images of the future contain valuable insights but they are constrained by two main problems: lack of recognition of ongoing social and technological developments and simplistic conceptions of privacy based on a dichotomy of the individual and society. A monolithic society is seen either as a threat to privacy or as the protector of privacy. Due to these problems, images of the future tend to be either fatalistic images which view individuals as helpless in the face of unstoppable loss of privacy or utopian images which neglect path-dependent technological developments and the difficulty of protecting privacy in a fragmented society consisting of many normative circles. Therefore, I will argue that one solution is a responsible attitude towards the future which takes present challenges seriously and views privacy as an institution that maintains social freedom in the context of normative intersectionality. Awareness of images of the future and of their assumptions is also important because it enables reflexivity and the dialogue of images of the future. Throughout, I maintain that non-experts' images of the future are important because they influence the actions of individuals and groups and therefore they affect the future of privacy.

1.1 Structure of the Thesis

This study contains two main parts: a theoretical part and an empirical part. First, I will discuss the theoretical tools which will be used in the empirical part. The study is set within the framework of critical futures studies and critical realism. Then, I will discuss the theoretical concept of image of the future and causal layered analysis as the method of analysis. Next, the foundation for the empirical part will be laid by developing a conception of privacy suitable for this study. This entails discussing central theoretical contributions to the topic of privacy. I will argue for a critical realist perspective that views privacy as a social institution which consists of norms concerning information flows and access to individuals. From this perspective, privacy is a structural feature of society rather than a mental state or a phenomenon constructed through language, for instance. Drawing on the work of Nissenbaum, Schoeman, Elder-Vass and others, privacy is conceptualised as a social institution for creating, maintaining and negotiating the boundaries between normative circles. Moreover, a preliminary model will be developed to explain changes in privacy. The model considers central elements of how privacy changes through the privacy-threatening practices of actors.

The empirical material for the study is provided by three focus group sessions held in spring 2012 in three countries: Finland, Germany and Israel. The focus groups were held as part of the PRACTIS project and they consisted of non-experts from various backgrounds who answered four rounds of open questions, each approximately 30 minutes in length.[1] In the empirical part, the focus group discussions will be analysed based on themes which draw on the theoretical model as well as the literature on privacy. The aim is to grasp individuals' privacy-related beliefs about the present and the past as well as about causes and effects. I will argue that the focus group participants can be divided

[1] PRACTIS (Privacy – Appraising Challenges to Technologies and Ethics) was project funded by the European Commission's 7th Framework Programme for Research and Technological Development and coordinated by the Interdisciplinary Centre for Technology Analysis and Forecasting at Tel Aviv University, Israel. See http://www.practis.org/.

into four clusters: privacy fundamentalists, privacy pragmatists, privacy individualists and privacy collectivists. Ideal-typical images of the future of these four clusters will be built and then analysed using the causal layered analysis method. Finally, the conclusion will summarise the findings and suggest their wider implications.

1.2 Assumptions

The approach taken in the thesis is based on three central assumptions or theoretical starting points. The first assumption is that in an analysis of images of the future, privacy should be seen as a *social and contextual phenomenon*. Adopting a social and contextual perspective on privacy means that privacy is viewed as a feature of societies rather than only a mental state of the individual or a universal value, for example. The contextual nature of privacy also means that privacy is a *dynamic* phenomenon which has different forms in different contexts and at different historical periods.[2] Privacy is also contextual in the sense that it is experienced within a micro context such as the home, workplace or a health centre. Because of this contextual nature, privacy is a challenging topic for a future-oriented study. The context-bound nature of privacy means that one cannot define privacy precisely and conclusively and then study its development into the future as one can with precisely defined variables such as the GDP of a nation-state. A decontextualised, unhistorical account of privacy would arguably be a case of privacy fetishism, seeing a human-created phenomenon as a natural one (Fuchs, 2011, p. 226; Lobet-Maris, Grandjean, Colin, & Birnhack, 2012, p. 47). Instead, privacy should be seen as a moving target. The particular forms which privacy takes change along with changes in technology and society, and they may even change differently in different contexts such as healthcare and policing. However, I will argue below (section 3.3.2) that there is a general *form* of privacy as a social phenomenon that is relatively constant.

The second assumption is that individuals' images of the future matter for the future of privacy. This assumption is related to the general premise of futures studies which states that futures thinking is vital for human action (Bell, 1997, p. 142). Images of the future are not only interesting in themselves but also because they influence the behaviour of individuals and groups.

[2] Privacy could also be seen very differently. Räikkä (2007, p. 29), for instance, argues that if privacy is taken to mean the inner life of the individual, it is not appropriate to examine changes in privacy. Clearly this approach would be less useful for futures studies.

The third assumption is that new and emerging technologies have a role in the future developments in privacy but they do not determine the future of privacy. As I will argue in section 3.4.2, I adopt a position of technological realism which sees technology as a force in creating path dependencies and possibilities, for example, but technology is not a social actor and its actual influence is tied to actors and their interests. Technology is seen neither as a determining influence on the future (technological determinism) nor as a purely instrumental tool that can be used for any purpose (technological neutralism). Technology gives *affordances* for privacy violations, but actors and their interests play a crucial part in determining to what extent this potential is used. On the other hand, people can actively appropriate technologies as well as find ways of avoiding privacy violations or adapting to them. The interests of actors and power relations play a key role in how the influence of technology comes into effect.

1.3 Research Questions and Hypotheses

In this study, the main topic of the futures of privacy is divided into research questions on three topics: privacy as a social phenomenon, privacy perceptions and images of the future of privacy. The main questions and sub-questions I will aim to answer are the following:

1. **What is privacy as a social phenomenon and how does privacy change over time?**

The first research question relates to the definition of privacy and to changes in privacy. From the social perspective, what kind of phenomenon is privacy? What functions does it have? What is it that changes when we say that privacy changes over time? Which factors cause the changes? Answering these questions will require a literature review of central theoretical writings on privacy and building a preliminary conception of privacy and an analytical model of privacy dynamics. My hypothesis is that such conceptions of privacy and of privacy dynamics can be found which enable a study of images of the future of privacy.

2. **How is privacy perceived among non-experts and which factors are seen to threaten privacy?**

The second question concerns the perceptions of privacy among citizens. The starting point is that concerning privacy, the views of ordinary citizens are important. Privacy is a topic that is notoriously difficult to define and it is closely linked with everyday experiences of people. The protection of privacy also depends partly on individuals. Therefore, it is important to be concerned with the kinds of information that non-experts can provide on the topic. Nevertheless, an understanding based on the scientific literature on privacy is also needed to set the views of individuals into context.

There are several sub-questions that help in examining privacy perceptions. Firstly, there are general questions concerning privacy. How do individuals define privacy and the functions of privacy? In what kinds of situations and contexts is privacy important? Secondly, there are questions relating to privacy threats. If privacy is seen as being under threat, what are viewed as the main threats to privacy? What kinds of actors and interests would threaten privacy? Who is ultimately responsible for protecting privacy? How can privacy be protected?

My hypothesis is that views on privacy can be grouped into clusters of similar views which represent ideal-typical conceptions of privacy. I will not claim that individuals with different privacy conceptions constitute self-conscious social groups but they do share assumptions and beliefs which are influenced by certain aspects of the cultural environment. The aim is not only to discover and describe such groups but also to systematically examine the underlying assumptions behind the beliefs about privacy.

3. What types of images of the future of privacy are there among non-experts with the time frame from the present until the year 2050?

The third research question relates specifically to the futures of privacy. It links with the first two questions which try to answer what privacy is and what threatens it. The first question deals with objective aspects while the second question deals with subjective perceptions. The first two questions, then, specify the topic and perceptions of it, and the third question is concerned with the futures of that topic. The time frame reaches from the present until the year 2050. From a policy perspective, the time frame is rather long but within futures studies such time frames are not unusual. The relatively long time frame is justifiable by the interest in critically examining alternative futures and not merely considering futures that seem probable at the moment. If the time frame were defined very close to the present, the space of possible futures would be much narrower, limited by current institutional arrangements and patterns of thought. With a longer time frame, there is more room for imagination and creativity in envisioning alternative futures. There are of course drawbacks to this approach. The long time frame makes the consideration of probable futures very difficult. Not much of value can be said about the year 2050, especially concerning such a fast-moving area as technology. The flipside of the increased imaginative possibilities is that the subjective way of perceiving certain social circumstances could be different in the relatively far future, which further complicates the study of alternative futures.

My hypothesis regarding images of the future is that conceptions of privacy and beliefs about the future of privacy are linked in a relatively systematic way in the sense that there is a logical connection between beliefs about privacy and images of the future of privacy. The first research question will be answered using literature on privacy, and the second and third research questions will be answered using the empirical focus group material.

1.4 Delimitations of the Study

In this section, I will delimit the approach to privacy that is taken in this thesis. Since privacy is such a multifaceted phenomenon, it must be approached from a particular perspective in order to cope with the amount of literature in any depth and to reach interesting results. Privacy will be approached here from the social point of view. Figure 1 illustrates the different aspects of privacy in a simplified way.

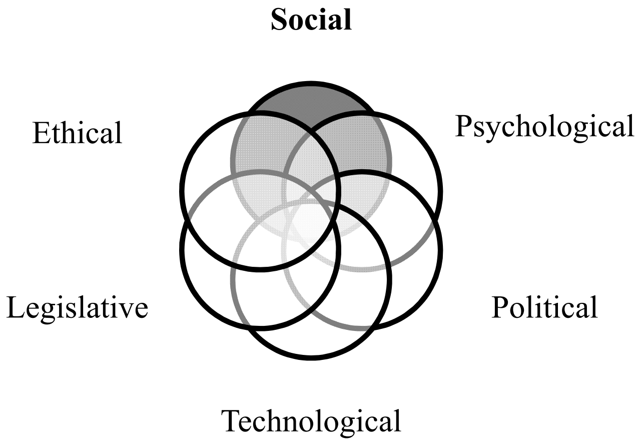

Figure 1 Different aspects of privacy

The diagram above is a heuristic illustration of different facets of privacy. The different aspects are perhaps best understood as different ways of approaching privacy. For example, approaching privacy from a social point of view draws attention to different questions than if one is interested in the psychological point of view. Illustrating the aspects of privacy as a Venn diagram also demonstrates that the different aspects of privacy overlap in various ways.[3]

In order to delimit the area of study, it is useful to briefly describe the aspects of privacy which are not the topic of this study. The psychological dimensions of privacy include aspects such as the functions of privacy for psychological wellbeing or cogni-

[3] In addition, the illustration raises the question whether privacy has a core which concerns all the different aspects. This question cannot be solved within the space of this thesis.

tive performance. Technological questions related to privacy concern the design and use of information systems, for instance. Ethical aspects of privacy include questions such as the foundation of the value of privacy and ethical justifications for ways of protecting privacy. The political dimension of privacy involves questions such as the link between privacy and democracy. Is privacy necessary for a functioning democratic system (e.g. the secret ballot), and inversely, is democracy necessary for preserving privacy? Moreover, issues of power and surveillance largely fit into this perspective, even though power can also be examined from a sociological point of view. Finally, the legislative approach considers privacy from the viewpoint of jurisprudence and deals with questions such as how privacy should be defined in legislation and which institutions and frameworks should protect it.[4]

The final three systems (ethics, politics and legislation) will be touched in this study, but only in connection with social aspects of privacy. In general, these issues of psychology, ethics, technology design, politics and legislation are not studied in this thesis as such, although interpretations and understandings of them that were presented in the focus group discussions are examined. For instance, focus group participants' beliefs about appropriate privacy legislation will be discussed and analysed, but my aim is not to present detailed law and policy recommendations as this would be the topic of another study.

In this thesis, privacy is studied from the social perspective. It is assumed that privacy is essentially a social phenomenon or at least that the social aspect is one central aspect of privacy. Privacy relates to how people interact with others and how they relate to the wider society, and privacy as an institution is also an aspect of social structure. The social perspective on privacy does not ignore the individual but it tries to go beyond the common definition of privacy as atomistic individuals escaping from the influence of society.

Adopting a social view on privacy does not mean denying the importance of studying privacy in relation to governmental surveillance, for instance but this is not the main focus from this viewpoint. The social perspective on privacy is general in the sense that many actors can potentially threaten privacy. Gavison (1980/1984, p. 357) argues that most privacy claims are not in fact for non-interference by the state but for interference by the state to protect against other individuals. In addition to the state, then, other individuals can be threats to privacy, as Mika Mannermaa (2007) argues by using the concept 'some brother' rather than Big Brother. Emphasising the social rather than political

[4] In addition to these six dimensions, one could of course suggest others, such as economic, organisational or cultural perspectives. As mentioned above, the dimensions are listed here for clarifying the perspective of this thesis.

aspects of privacy also does not mean ignoring issues of power. Instead, it means that power is viewed from a sociological viewpoint rather than focusing on formal political power held by branches of the government and other public actors.

A few general delimitations are also in order. The issue of cultural differences in privacy perceptions and privacy protection is an interesting issue but it is beyond the scope of this study. The present study will in effect limit itself to the Western context, although my definition of privacy as a social institution allows the possibility that this institution takes a different form in different cultures. In addition, I provisionally agree with Daniel Solove's (2008, pp. 183–187) contention that while conceptions of privacy are culturally contingent, the underlying problems related to privacy are similar in most industrialised societies with an economy that is heavily based on information. The preferred solutions may differ, but the problems are generally similar. Moreover, with increasing globalisation, there is likely to be more convergence than divergence in this regard.

Additionally, this thesis will not deal with the issue of organisational privacy, meaning for instance data protection which protects information belonging to an organisation. My definition of privacy, however, suggests that organisational privacy, in this meaning, is perhaps best considered under some other title such as secrecy or intellectual property because the functions of privacy are linked so closely to individuals. Organisational privacy, then, could mean protecting the data of *individuals* within organisations, for instance.

Quantification of privacy and quantitative predictions concerning the level of privacy are also excluded from this thesis. Any models that I present are purely qualitative. Although quantitative approaches may provide valuable information, they tend to radically simplify the multi-dimensional phenomenon of privacy. However, it is possible that at some point theories of privacy as a social phenomenon will be formalised to the extent that useful quantitative models can be formulated.

1.5 Originality of the Thesis

Privacy is clearly a much discussed issue in academic literature and a thesis on privacy must somehow justify its contribution to this literature. While there is a great deal of academic literature on privacy, there is less literature focusing on the futures of privacy and, to my knowledge, none dealing with images of the future of privacy. Some authors make brief references to the future of privacy. At the very end of Daniel Solove's *Understanding Privacy* (2008), the author notes that new technologies will continue to bring forth new privacy problems and transform existing ones. He argues that a clear framework such as his own is needed for an understanding of privacy problems, so that privacy can be balanced with countervailing interests (2008, pp. 196–197). Juha Räikkä also makes a passing mention of the future of privacy when discussing genetic privacy in particular. According to Räikkä (2007, p. 159), the discussion on genetic privacy will continue and widen to new situations and new value questions, because of the progress of medicine and the increasing number of applications of genetic data. However, these mentions include no substantial discussion of the future of privacy.

Other authors present more substantial scenarios about the future of privacy. David Brin (1998, pp. 296–300) outlines four negative surveillance scenarios: surveillance elites, surveillance obsession, surveillance acceptance and surveillance overload. However, on the whole Brin presents a highly polemical account in favour of transparency and he views privacy narrowly as the right to be let alone (1998, p. 334).[5] Therefore his account is not directly useful here. Within the field of futures studies, Mika Mannermaa has touched the topic of privacy in discussing life in ubiquitous information societies. His central thesis is that surveillance is currently exercised by a semi-invisible and diffuse 'some brother' consisting of public and private actors as well as individual citizens. Privacy is thus threatened not only by governments and companies but also potentially by anybody and for various reasons. According to Mannermaa, 'some brother' controls, knows and never forgets. Mannermaa presents three negative surveillance scenarios based on the dominance one of three powers: the state, the market and civil society. He argues that a benign scenario would be one where all three powers work efficiently (Mannermaa, 2007, p. 111, 2008, pp. 34–36). The crucial change for Mannermaa is the increasing ease and democratisation of surveillance. This democratisation is clear today from the proliferation of camera phones, for example. However, neither Brin nor Mannermaa engage with the conceptual work on privacy and their work is mainly useful for the discussion of threats to privacy.

Research projects funded by the European Commission have also built privacy scenarios. The SWAMI project developed four "dark scenarios" with reference to data protection in the context of ambient intelligence (Hert, Gutwirth, Moscibroda, Wright, & González Fuster, 2008).[6] In addition, five general privacy scenarios were created within the PRACTIS project from which the focus group material for this study was acquired. These scenarios were based on expert interviews and they discussed the possible futures

[5] Moreover, I would use 'transparency' in a different sense than Brin who connects it with the openness of individuals. For me, transparency means the openness of organisations towards citizens. While institutions should be transparent in a democracy, individuals arguably have no such duty.

[6] SWAMI (Safeguards in a World of Ambient Intelligence) was a project funded by the European Commission's 6th Framework Programme for Research and Technological Development.

of privacy based on different assumptions about social, political and other changes (Auffermann, Luoto, Lonkila, & Vartio, 2012). The central aim of these scenario efforts was to formulate policy and legal implications and the approach was quite different from this thesis where the focus is on images of the future that are presently held by non-experts. Comparing the results of these two approaches could be fruitful but it is not attempted in this thesis.

It could be argued that there is a research gap in future-oriented studies of privacy as a social phenomenon. To my knowledge, none of the existing literature deals with images of the future of ordinary citizens, on the one hand, and with the social perspective on privacy, on the other hand. Therefore this study has originality value. On the other hand, the conclusions of this study, particularly on the images of the future of privacy, must be provisional and cautious since there are no prior studies on the topic. Additional research, including empirical research, is needed in order to reach more certain results.

This thesis is primarily an academic work aimed at furthering the understanding of privacy and various futures of privacy. However, the results may also have practical value for several purposes. Firstly, they illuminate the hopes and fears of the public that are related to privacy in the future. These attitudes should be taken seriously by designers of information systems, for instance. Similarly, governmental actors and companies should also consider the experiences and attitudes of individuals because these attitudes affect the behaviour of individuals. On the other hand, educators and education planners need to assess whether awareness about privacy should be raised, and citizens' images of the future can provide material for this consideration.

This study also features a unique combination of methods and research material. Combining focus group data with causal layered analysis is expected to yield valuable results that can draw on the strengths of both methods, while the combination of the two provides unique advantages that neither methodology alone would provide. The focus group data collection method benefits from causal layered analysis because CLA provides a systematic method for analysing the data. In turn, the causal layered analysis benefits from the fact that there is empirical material to analyse.

2 FUTURES STUDIES: THEORETICAL APPROACH AND KEY CONCEPTS

This thesis is set within the overall framework of critical futures studies which focuses on critically examining the present and exploring alternative futures. I will argue that critical futures research, viewed from a critical realist perspective, should emphasise the openness of the future but also acknowledge ongoing social processes and the limits of social construction. After a discussion of critical futures studies, the central concept of image of the future will be examined. I will discuss how images of the future can be used as conceptual tools in discussing the futures of privacy, in particular. Then, causal layered analysis will be presented as an interpretive framework for analysing images of the future of privacy. I will argue for an application of causal layered analysis based on critical realism as opposed to the poststructuralism suggested by Inayatullah (2004a).

2.1 Critical Futures Studies, Critical Realism and the Open Future

The meta-theoretical approach that is taken in this thesis is critical futures studies combined with a critical realist perspective. My starting point for critical futures research is Bell's (1997, pp. 181–183) view of futures studies as an action science and a transdisciplinary social science. Futures research requires many kinds of knowledge but awareness of social theory is crucial for studying, and perhaps promoting, social change processes.

Sohail Inayatullah and Richard Slaughter have argued for a radical approach to critical futures research which has some strengths but in my view it must be supplemented with a critical realist framework. Inayatullah distinguishes critical futures studies from predictive and cultural futures research. According to him, the critical futures approach is focused on making the present remarkable by problematising current categories (Inayatullah, 2004b, p. 71). Richard Slaughter, in turn, distinguishes critical futures studies from what he terms 'pop futurism' and 'problem-oriented futures work'. Pop futurism refers to non-theoretical popular work which often features predictions about technology. Problem-oriented futures studies refers to a large part of mainstream futures research which deals with the challenges that are likely to emerge in the future. Critical futures studies, in contrast, aims to understand the processes of "meaning-making, paradigm formation and the active influence of obscured worldview commitments". This understanding enables the search for alternative futures. Critical futures studies examines social structures, trends and problems as social constructions that can be questioned and renegotiated (Slaughter, 2004, pp. 148–149). The preoccupation of critical futures studies is thus on opening the future to alternatives by questioning current understandings of the future and of change processes. The assumption is that there are, as Slaughter (2004, p. 148) puts it, "[v]astly more choices than ever seriously explored".

The strength of critical futures studies is that it takes into account power, interests and the symbolic construction of the social world instead of only focusing on problems as they are commonly understood. Foresight and planning activities often involve a use of power because the future is contested and much more uncertain than the present and because many interest groups are struggling for power to influence the future. As Inayatullah (2004b, p. 77) notes, many power interests are embedded in forecasts and in the language in which they are written. Futurists should thus be conscious about their power and ethical responsibility when they are giving recommendations based on foresight. Within scenario building, for instance, futurists should be explicit about why particular drivers are chosen and how variables are altered to produce different scenarios.

As an object of study, futures should be approached differently than the past or the present, and critical futures studies arguably acknowledges this difference more explicitly than empirical and positivistic approaches. The first crucial difference is that for the past and present, there is empirical material on which interpretations can be based. There are always various research interests and multiple interpretations of history and of present reality, but at least in theory these can be tested for consistency with empirical data which have been collected with systematic and transparent methods. In contrast, studying the future is a very different matter. Bertrand de Jouvenel already made the distinction between *facta* and *futura* in the 1960s, and it is a widely accepted premise of futures studies that the future is nonevidential and there are no future facts (Bell, 1997, p. 148; de Jouvenel, 1967, pp. 3–6). Strictly speaking, there are no empirical data about the future. Instead, there are different kinds of projections: trend extrapolations, scenarios, visions and images of the future. Since there are no data, unverifiable beliefs and hopes about the past and the present as well as stories about the future play a particularly important role in futures studies. It has been plausibly argued that futures studies should include a cultural studies component since futures are told as stories with a particular structure, and it is important to examine the cultural structures on which the construction of myths is based (Patomäki, 2006, pp. 26–27). Tools such as causal layered analysis are useful for examining these cultural understandings.

The other crucial difference between the future and the past or the present is that the future can still be influenced. In addition to the nonevidential nature of the future, an equally important premise of futures studies is that the future is not totally predetermined (Bell, 1997, p. 150). Therefore, there is not one future but many possible, probable and preferable futures. However, critical futures studies in Inayatullah's and Slaughter's sense can be criticised for overemphasising the openness of the future. Slaughter, for example, uses rather extreme language in describing the critical futures position: "All structures are provisional. They can be problematised, re-framed, reconceptualised, deconstructed and, on the other hand, rechosen, re-conceptualised, and so on" (2004, p. 157). This position is similar to social constructionism where social phenomena are seen as discursive constructions and social change is framed in terms of change in discourse and conceptualisation (Alvesson & Sköldberg, 2009, p. 23). The question can be raised whether social life truly is so radically free and re-negotiable. A realist counter-argument would be that there are objective social structures, mechanisms and processes which are very difficult if not impossible to restructure. Certainly changing the way we speak about them will not be enough to change them. The future is also path-dependent: there are past and present events and processes which are making certain futures much more likely than others (Adam & Groves, 2007, p. 172).

Adam and Groves criticise De Jouvenel's facta/futura distinction for three reasons. Firstly, the distinction fails to recognise factual processes that are in motion in the present but have not yet materialised into empirical phenomena. Secondly, the distinction views the future as an empty vessel to be filled, while in reality the future is always already partly filled by the decisions and actions taken in the past and the present. Thirdly, the facta/futura dichotomy makes no distinction between *present futures* (futures understood from the perspective of present categories, as abstract imagination or as potential profits to be made) and *future presents* (the present in which future generations will live and which is filled with the consequences of choices made in the past) (Adam & Groves, 2007, pp. 36–37, 196, 200). There are thus real processes which are already happening and which will have an effect on the future independent of our visions or images of the future. This does not mean that these processes cannot be affected, but the point is that they are not mere discursive constructions or mental images. The future does not yet exist but there are possibilities for the future and present processes which affect the future. As Bell (1997, p. 226) argues, there is conjectural or surrogate knowledge about the future: justified belief in statements about the future.

Studying the future thus involves two main aspects: firstly objective social and natural processes which are already in motion and which are alterable within limits, and secondly our presently existing and culturally conditioned stories of alternative futures. It is important to distinguish between these perspectives on the future: the first deals with real possible futures, however difficult it is to consider the possibilities, while the second deals with how the future is viewed today. In Adam and Groves's terminology, the first perspective is that of future presents and the second perspective concerns present futures. They could also be termed objective and subjective futures, respectively.

How can these two views of the future be reconciled for the purposes of this study? I would argue that the study of futures could be viewed as the dialectic of objective and subjective futures. Critical and reflexive futures research should deal with both aspects to some extent and researchers should make clear which aspect they are discussing at each time. In this study, I will discuss *images of the future* which are subjective mental images or shared cultural images which do not necessarily represent real social processes realistically. Causal layered analysis is used to study these cultural images of the future. In this sense, my focus is on subjective present futures. However, images of the future also have an objective dimension because they have real social consequences. Images of the future as well as individual and cultural beliefs affect the behaviour of people and groups and thus contribute to social change.

It could be said, then, that the social world is partly symbolically constructed but it is constructed within certain limits that are not freely alterable, at least within a short time frame. In addition, the social world is constructed through the interaction of individuals, not only through use of language, and therefore merely understanding it differently is not enough for changing it. Change happens when a new understanding leads to action by individuals or groups.

De Jouvenel and Inayatullah present important conceptual tools for examining the openness of different aspects of the future. De Jouvenel divides futures into dominating and masterable parts. The masterable future is something which can be changed by human action, while the dominating future cannot be changed. Importantly, the dominating and masterable parts are dependent on the agent in question. De Jouvenel argues that futures which are dominating for individuals may be masterable for more powerful agents such as an organisation or the government (1967, pp. 52–53). The dominating/masterable division helps to examine the openness of future presents, in Adam & Groves's terminology.

Inayatullah's layered methodology is also useful in considering the limits of restructuring, since the different layers correspond to different time frames that are needed for changing them. The deeper layers are slower to change because they concern deeply held value commitments (Inayatullah, 2004a, p. 16). The layered methodology is particularly useful for examining the openness of present futures, that is, for investigating the malleability of current cultural understandings of the future. If they influence behaviour, these subjective understandings will ultimately influence objective futures. However, Inayatullah's methodology must be adopted with certain reservations, which are discussed in the section on causal layered analysis.

In my view, critical futures research can account for the subjective-objective futures dialectic by being combined with a critical realist framework. Critical realism has been proposed, in different versions, as both an epistemology and an ontology for futures studies (Bell, 1997, pp. 207–238; Patomäki, 2006). For epistemology, critical realism means acknowledging the influence of historical context and human interests and biases as well as the fallibility of scientific knowledge but nevertheless insisting that scientific knowledge can approach truth (Bell, 1997, pp. 207–209). Bell's belief in the approximation of truth by science and rational argumentation is close to what Karl Popper (1945/1966, pp. 225, 229–231) called critical rationalism.

In general, Bell's critical realism is a fruitful epistemological perspective for futures studies. However, I do not agree with Bell's contention that with enough knowledge, value judgments can be made objectively using models such as Keekok Lee's epistemic implication model (Bell, 2003, pp. 87–110). While science can provide knowledge for assessing the desirability of futures, it is in my view exaggerated to claim that scientists or other foresight professionals can make final value assessments (cf. Tapio, 1999, pp. 89–93). On the issue of values, my position is more relativistic and pluralistic than Bell's moral objectivism. Using Tapio and Hietanen's (2002, pp. 602–608) typology, my position is closer to pluralistic humanism and critical pragmatism than Bell's optimistic humanism.

From the ontological perspective, critical realism gives a scientific foundation to the notion that there are alternative futures although there is a reality outside any interpretations of it. According to critical realists, actual, empirically observable events are only one part of the reality which also includes present possibilities and powers of existing structures as well as social mechanisms that give actors causal power. Furthermore, social structures are reproduced by social action and therefore they may be transformed and new structures may emerge (Bhaskar, 1979/2003; Patomäki, 2006, pp. 9–10). Crucially, ideas and discourses are among the factors which can have causal effects (Alvesson & Sköldberg, 2009, p. 41). In this sense, reality is socially constructed.

A mechanism-based approach, such as the approach of critical realism, makes prediction problematic, because mechanisms are not exceptionless laws and phenomena are always caused by multiple interacting forces (Elder-Vass, 2010, p. 47; Hedström & Ylikoski, 2010, p. 55). Nevertheless, something can be said about future possibilities because causal mechanisms inherent in structures are more stable than the surface level of events. From this perspective, it is important to acknowledge the existence of latent phenomena which exist as possibilities but which have not been realised because some other crucial factors are not present (Karlsen, Øverland, & Karlsen, 2010, pp. 66–67).

Critical realism, then, supports the notion of critical futures studies that the future is open within certain limits. Combined with Inayatullah's approach to studying cultural understandings, critical realism presents a robust starting point for researching both objective and subjective futures. This approach admits the possibility of an increasingly accurate description of currently held images of the future and of the mechanisms and processes affecting futures, but it also acknowledges that futures are told as stories which are influenced by cultural understandings. Science cannot reach certain knowledge about futures and it cannot solve value debates, but nevertheless rational argumentation regarding future possibilities is preferable to cultural relativism. As a broad research approach, critical realism represents an alternative to positivism and social constructionism (Alvesson & Sköldberg, 2009, p. 39). In the context of futures research, it represents a middle ground between predictions which take social structures as given and the assertion that the future is completely open for restructuring.

2.2 Images of the Future

According to Wendell Bell, the image of the future is one of the central concepts of futures studies. Bell states that studying images of the future is a field where futurists can operate as basic researchers (1997, pp. 81–82). According to Bell and Mau's working definition, an image of the future is "an expectation about the state of things to come at some future time." For Bell and Mau, these expectations are better seen as a range of possibilities rather than points on a continuum (1971, p. 23). An image of the future is essentially a description of one possible future.

Images of the future can be contrasted with scenarios, on the one hand, and visions, on the other hand. Images of the future differ from scenarios in two key aspects. Firstly, they focus on one point in the future, while scenarios outline the *process* of how the future state comes into being. Secondly, images of the future can be seen as mental images that are presently held by individuals rather than being constructed by researchers and experts. On the other hand, scenarios and images of the future are similar in the sense that both emphasise the plurality of the future: there are many alternative images of the future and many possible scenarios about the future. The main difference between images of the future and visions is that the concept of image of the future emphasises exploring and analysing a particular future, while the main task of visions is to inspire and give direction (van der Helm, 2009, p. 100n).

Images of the future can differ from one another on many dimensions. They may be short-term or long-term, individual or shared, simple or complex, desirable or undesirable, consciously or unconsciously created and weakly or strongly held, among other things (Bell & Mau, 1971, pp. 23–24). Images of the future may also be images of the future of a geographical unit such as a state or of a particular institution (Bell, Mau, Huber, & Boldt, 1971, p. 52). This last point is important for my study because in the next chapter I will define privacy as a social institution. This study is then an examination of images of the future of privacy as an institution.

Images of the future are important for two related reasons. Firstly, it is arguably a psychological need of individuals to make the future more understandable by creating images of what the future might look like. Through a partly subconscious process, individuals make conjectures about the future based on beliefs and knowledge about the past and present (Rubin, 2013, p. S40). Individuals and groups need these expectations of the future in order to make everyday decisions as well as more far-reaching ones (Bell, 1997, pp. 142–145).

Secondly, images of the future are important because they shape people's actions in the present both consciously and unconsciously. According to Bell (1997, p. 82), many futurists share this theoretical notion. Boulding (1956/1963, p. 18) argues that an adequate theory of behaviour must take individual and shared images into account. For Boulding (1962, p. 193), the behaviour of an individual in the present "depends very largely on the quality of his image of the future", whether it is an optimistic or pessimistic one. Both Inayatullah (2008, pp. 7–8) and Polak (1955/1973, p. 1) view images of the future in terms of the *pull of the future*. Shefrin (1986, p. 208) argues, perhaps exaggerating, that images of the future can be "agents of cultural change" influencing actions, attitudes and institutions. Images of the future are thus mainly important because of their consequences. They influence the actions of individuals and groups and therefore they play a part in shaping the future.

Bell and Mau have formalised the role of images of the future in social change into a diagram which is reproduced below.

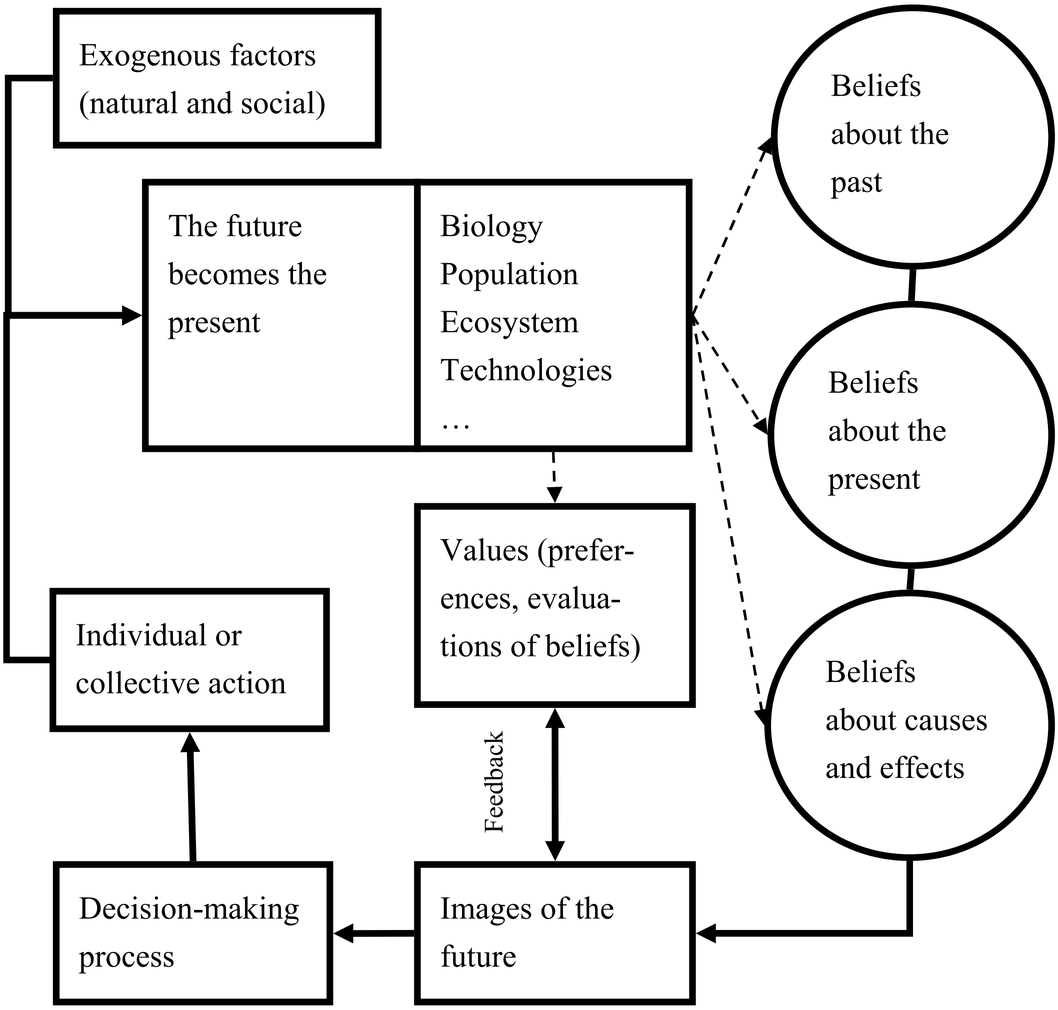
Exogenous factors (natural and social)
The future becomes the present
Biology
Population
Ecosystem
Technologies
…
Beliefs about the past
Beliefs about the present
Beliefs about causes and effects
Values (preferences, evaluations of beliefs)
Individual or collective action
Feedback
Decision-making process
Images of the future

Figure 2 Model of social change according to Bell and Mau (1971, p. 21)

In their model, Bell and Mau present a kind of social mechanism through which images of the future influence the future. Two critical aspects produce social change: social action and factors which are exogenous to the model. Social action stems from decision-making which in turn is affected by values, beliefs and images of the future. Bell and Mau's model emphasises rational decision-making but they also acknowledge that decisions may also be made less consciously (Bell & Mau, 1971, p. 24). Rubin (2013, p. S40) emphasises imagination and the hopes and fears of individuals in addition to cognitive beliefs in the formation of images of the future.

The strength of Bell and Mau's conceptualisation is that they provide the individual-level mechanism through which images of the future affect the forming of the future rather than merely writing about an abstract pull of the future. This differentiates images of the future from utopias with no connection to social reality. In effect, images of the future become real because they affect the actions of individuals and groups, that is, they have real social consequences.[7]

In this thesis, I will not study the mechanisms of decision-making and action through which images of the future have social consequences. It will be assumed that images of the future are both intrinsically of interest and that they have social consequences. The focus in this study is on the right-hand side of the diagram: on beliefs, values and images of the future. The causal layered analysis approach helps, in particular, to examine the connection between values and beliefs about the nature of reality. In the CLA approach, beliefs and value commitments are organised into mutually supportive layers. Beliefs about the past and present may concern several CLA layers, depending on whether they are litany type of beliefs adopted from the media, systemic beliefs or more deep-rooted beliefs. Beliefs about causes and effects mostly concern the system layer of CLA, and values mostly concern the worldview and myth layers. Images of the future, in turn, can be examined using all of the CLA layers.

A further issue is the question of shared images of the future and the influence of culture in general. It can be argued that in forming their beliefs, values and images of the future, individuals are influenced but not determined by the social groups to which they belong. Furthermore, individuals need not be aware of the particular image of the future and all its implications but they may still be acting under its influence. It can be argued that images of the future affect the future both through a conscious striving for or against a particular future and through largely unconscious processes influenced by the normative beliefs shared by a particular group. Images of the future are thus linked to

[7] An area of study that cannot be discussed here is the cognitive psychology of images of the future, that is, empirical research into how individuals process images of the future.

groups in complex ways, and Bell and Mau's model is not explicit about the formation of shared images of the future and the role of individual and shared beliefs.

Frederik Polak's account, on the other hand, focuses on societal images of the future. In his classic work *The Image of the Future* (1955/1973), Polak was explicitly interested in shared public images of the future, not private ones. Polak (1955/1973, p. 14) believes that the operational principles are the same for both types of images. Polak (1955/1973, p. 5) views shared images of the future as a "propelling power", that is, a powerful driving force of societal development. For Polak, the "*rise and fall of images of the future precedes or accompanies the rise and fall of cultures*" (1955/1973, p. 19, emphasis in the original).

However, Polak's approach can be criticised on two accounts. Firstly, Polak promotes an understanding of social change that is based on philosophical idealism as opposed to materialism. In this view, ideas rather than social actors are primary drivers of change which shape societies. Boulding (1962, p. 193) argues that Polak ignores latent processes which operate independently of the conceptions of people participating in them. These processes are also important, although truly latent processes are difficult to identify in practice (K. E. Boulding, 1956/1963, pp. 116–117). This criticism is similar to the critiques of critical futures studies outlined in the previous section.

Secondly, Polak's argument is simply too broad to be scientifically assessed. His argument sweeps across historical periods and the use of theoretical terms is arguably more suggestive than systematic. Polak arguably presents hypostatised collective images of the future without accounting for how these images are formed. These features make Polak's account difficult to reconcile with a critical realist perspective which is focused on discovering the real entities and mechanisms that cause social change.

The approach to images of the future should be explicit about moving between levels of analysis from the micro level of individuals to the macro level of societies. First, there is no necessary reason that images of the future function similarly on a societal level as compared to the individual level, that is, that they would be formed of societal beliefs and values and they would lead to collective action. Deriving an argument about shared images of the future based on individual images would be committing a fallacy of composition. Second, shared images of the future are not necessarily a sum of individuals' images.

In this thesis, I will attempt to solve the problem of grouping participants' views by using the sociological concept of ideal types. I will not claim that focus group participants with similar views are part of any self-conscious social group. Instead, I will characterise the common features of privacy conceptions and images of the future by using ideal types. An ideal type is a hypothetical characterisation of a phenomenon in its purest form that is aimed at capturing its essential features (Clegg, 2007; M. Weber, 1922/1978, pp. 18–22). The use of ideal types is arguably problematic from the critical realist perspective since they are subjective models created by the researcher rather than real entities. However, I would argue that the ideal type approach is appropriate for grouping the participants' perspectives and crystallising them as alternative futures. From a critical realist viewpoint, a hypothesis can be put forward that participants within different groups are subject to the influence of the same discursive norm circles, but this hypothesis cannot be tested in this thesis (Elder-Vass, 2012, pp. 153–157).[8] This notion is similar to Boulding's (1956/1963, p. 133) concept of subcultures as groups of people sharing a public image. In the empirical part of the thesis, then, I will discuss privacy conceptions and images of the future as ideal types. They are not held by any focus group participant in their ideal-typical form, but nevertheless the ideal types capture the essential features of privacy conceptions and images of the future.

From a critical futures studies perspective, images of the future are also linked to politics, interests and the use of social power. Within society there are many conflicting images of the future and some of these are deemed more socially acceptable than others (Rubin, 2013, pp. 40–41). Shefrin (1986, pp. 209–212) argues that dominant images of the future and the related values and assumptions are often intentionally kept concealed in the interests of efficient governance and the choice of images is narrowed, while democracy requires interaction and conflict between images of the future. Images of the future are thus not politically and ethically neutral but they may serve certain interests. However, this also means that consciously adopted alternative images of the future may be used for promoting desirable ends, especially if the images take real social processes into account. Patomäki (2006, p. 29) calls such images concrete utopias. Therefore, an awareness of images of the future as well as choice between alternative images should be promoted. This would increase individuals' ability to reflexively consider the assumptions behind their own decisions and the desirability of the connected images of the future as well as critically examine socially dominant images of the future.

Finally, I will discuss two criticisms of the notion of images of the future: criticism of philosophical idealism and the momentary nature of images of the future. Images of the future can be seen as linked to essentially an idealist conception of social change, where images, beliefs and attitudes are the drivers for social change. This is warranted if there is a notion that images of the future somehow by themselves cause social change. However, I have argued that images influence social change through the actions of individuals and groups. As Bell (1997, p. 93) states, images of the future provide the goals and motivation for designing social change, but their effectiveness depends on willing and capable people to put them to action. Therefore the change caused by images of the

[8] Normative circles will be discussed further in the analysis of privacy in section 3.3.2.

future has a material basis: the images motivate the social actions of individuals and groups.

Secondly, images of the future can be criticised for being momentary scenes from the future which ignore continuous change processes. In this sense, images of the future are very non-temporal and even unrealistic. Indeed, if something is certain about the future, it is that things will continue to change. Partly this criticism can be answered by juxtaposing images of the future with scenarios and noting that images of the future relate to subjective images held by individuals and groups and therefore they do not need to have a simple relation to real change processes. On the other hand, as Patomäki (2006, p. 7) stresses, individuals already view factual and possible events in terms of narratives with particular plots and characters even before the researcher makes her own narrative. Social actions have meaning in the context of this kind of narrative. Therefore, it could be more fitting to talk about narratives of the future, paths to the future or beliefs about the future rather than images of the future. Alternatively, one could speak of scenarios in Peter Schwartz's sense of the term. For Schwartz (1996, p. 36), scenarios are about subjectively "perceiving futures in the present" rather than predicting the future. The concept of images of the future is used here because it is an established part of the intellectual history of futures studies, particularly when discussing subjective understandings of the future. There is, however, the reservation that images of the future should not be seen as strictly momentary images but instead as subjective narratives about the future.

2.3 Causal Layered Analysis

Causal layered analysis (CLA) is the central methodological tool used in analysing the images of the future of privacy in this thesis. CLA is a method of studying understandings of the future by layering them into four layers: litany, system, worldview and myth (Inayatullah, 2004a, pp. 11–15). The strength of causal layered analysis is that it enables the study of individuals' socially and culturally influenced beliefs and the assumptions behind them. The epistemological aspects of CLA are discussed here and the methodological aspects are discussed in the empirical part in section 6.1.

For Inayatullah, causal layered analysis is rooted in the poststructuralist philosophy of Jacques Derrida and Michel Foucault and it utilises the tools of deconstruction, genealogy, distance, alternative pasts and futures, and reordering knowledge. In particular, deconstruction, which has its roots in Jacques Derrida's philosophy, is a central tool. In the CLA context, deconstruction is a method of 'unpacking' a cultural object or way of thinking and studying its internal logic and contradictions as well as the politics and assumptions behind it (Derrida, 1967/1997, pp. 10–18; Foucault, 1969/2002; Inayatullah, 2004a, pp. 8–10). In Inayatullah's view, CLA does not privilege certain ways of knowing such as scientific knowledge (2004a, p. 14). Instead, many different perspectives are taken into account in discussing plans or images of the future.

Causal layered analysis thus implies a rather radical philosophical position where all knowledge, including scientific knowledge, is ultimately seen as rooted in cultural beliefs about reality. As Inayatullah (2004a, p. 7) states, civilisational futures studies "informs us that behind the level of empirical reality is cultural reality (reflections on the empirical) and behind that is worldview (unconscious assumptions on the nature of the real)". He argues that the role of empirical research is "providing evidence of reality" but it must be complemented by considering the different layers (2004a, p. 10). According to Inayatullah's poststructuralist position, it is not only that knowledge of reality is mediated through language but language constitutes reality (2004a, p. 7). Interpreting this epistemological position strictly, all scientific theories could be viewed as evidence of a particular socially constructed worldview which is rooted in a deeper cultural reality. Theories of social structure, for instance, would be merely one cultural view of the social structure and their validity cannot be verified by any objective standard. However, Inayatullah's position differs from radical postmodernist relativism in that he views reality as vertically constructed, and each discourse has its place in this structure. This ontology is rooted in Indian philosophical thought which views the mind as constituted by layers or shells (Inayatullah, 2004a, pp. 4–5).

Does CLA then require the researcher to adopt a poststructuralist position towards all scientific research? I would argue that this is not necessary. Causal layered analysis has been described as a meta-method rather than a method because it does not dictate the methodological and theoretical approaches used in the analysis (D. L. Wright, 2002, p. 534). CLA can thus be combined with many different research perspectives. As I argued in the previous sections, I will adopt a critical realist standpoint which mediates between positivism and radical constructivism. While I agree with Inayatullah's contention that cultural beliefs are a part of the social world and therefore an object of study, I disagree with the argument that cultural beliefs are behind all knowledge about reality. In contrast to Inayatullah's view, I would agree with Bell that the task of science is to rationally approximate the truth while seeking awareness about one's own assumptions (Bell, 1997, pp. 171–173). In the case of studying futures, the openness of the future and the existence of many possibilities must also be taken into account.

CLA and critical realism are similar in the sense that both adopt a layered understanding of change, but the underlying ontology is different. I would interpret the layers of CLA as an analytical tool in understanding subjective perceptions of reality rather than claiming that reality as such is layered in this way. My view is essentially that social reality is complex and cannot be grasped or explained by any simple means, and analytical tools such as the layered structure of CLA are useful for understanding it.

However, this does not mean that reality itself is by necessity structured in this layered way.

Of course, the object of study influences the choice of theoretical and methodological approach. The researcher should acknowledge the difference between studying social structure and cultural objects, for instance. In my view, studying social structure and social change processes from a realist viewpoint is crucial, since not all features of social structure and change processes are rooted in cultural perceptions, even though understanding them is mediated through language and culture. On the other hand, images of the future can be studied as cultural objects, as texts, and here the understanding of beliefs, attitudes and myths is important. However, these cultural understandings should ultimately be related back to the real change processes as Bell and Mau do in their model (see p. 23). It is important to study the impact of stories about the past, present and future because these "structured and reflexive anticipations" of individuals and groups are a part of the social system (Patomäki, 2006, p. 17).

An important aspect of CLA is the assumption that the myth, worldview and social context layers in a sense create problems as they are seen on the litany level (Inayatullah, 2004a, p. 3). This is because these deeper levels affect how the problem is framed and conceptualised, and indeed, that it is seen as a problem in the first place. Problems are situated and seen as problems within a certain context that includes social interests, power relations and definitional power (Slaughter, 2004, p. 158). For instance, loss of privacy is only seen as a problem in a culture that values privacy, and privacy is only desirable in some social contexts (Schoeman, 1992, p. 114). Indeed, there are many potential negative effects of having *too much* privacy, including promoting individualism and harming the common good, legitimating domestic violence, planning and perpetrating illegal activities and consciously misleading others (Fuchs, 2011, p. 224). For David Brin (1998, passim), for example, reciprocal transparency is in many cases preferable to privacy protection. This also demonstrates why privacy is such a fruitful area of study: there are widely different views and ideologies around it.

In chapter 6, the focus group material will be analysed using the CLA layers. The ideal-typical images of the future will be mapped onto the CLA layers in order to analyse the assumptions behind them. The deeper worldview and myth layers require interpretation because they are generally not discussed explicitly in the focus groups. Before turning to the empirical material, I will formulate a conception of privacy as a social phenomenon in the following chapter.

3 THE CONCEPT OF PRIVACY: LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

The topic of this thesis is the future of privacy. Before images of the future of privacy can be explored, the concept of privacy must be defined somehow. Inayatullah writes that the task of critical futures studies is to problematise current categories and inquire into how problems are framed (Inayatullah, 2004b, p. 72). Therefore, privacy as a category must not be taken as a given, but it must be critically examined in order to understand how privacy problems are framed in academic and everyday debates and to understand the meaning of images of the future of privacy.

In this section, I will examine theories of privacy and develop a conceptual framework for this study. Engaging in a critical literature review on the concept of privacy is a daunting task. At first, it must be stated that there is no single agreed definition of privacy. Nissenbaum (2010, p. 67) states that the "landscape of theoretical work on privacy is vast, spanning disciplines from philosophy to political science, political and legal theory, media and information studies, and, increasingly, computer science and engineering", with the only consensus being that "privacy is a messy and complex subject".[9] Schoeman (1992, p. 11), in turn, argues that "nearly everything about privacy, from its scope to its value, is controversial". A further complication is that privacy is often seen as a dynamic and evolving concept (Tavani, 2008, p. 132). There are, however, some useful meta-theoretical overviews of classic definitions of privacy which will be discussed in the next section before turning to more recent theories of privacy and then to my own approach to privacy in this study.

There are several competing accounts of privacy with their inherent strengths and weaknesses. A central concern in studying privacy is to maintain conceptual focus while acknowledging the complexity of the phenomenon. An additional challenge is that in many theories of privacy, the foundational assumptions are not explicitly stated which makes assessing them more difficult. This task of critically assessing assumptions behind theories is nonetheless crucial from a critical futures viewpoint.

My approach to theorising privacy is guided by the central aim of this study: to explore images of the future of privacy. The approach to defining privacy is guided by this purpose but the definition of privacy is not viewed as purely instrumental for this purpose. The aims of the study outline the perspective to privacy, and then a tentatively

[9] To this list could be added the cross-disciplinary approach of surveillance studies, which views privacy issues from the perspective of surveillance practices (Lyon, 2007). Due to time and space restrictions, the field of surveillance studies will not be discussed in depth in this thesis.

true definition from this perspective is sought. Considering the aim of discovering images of the future, I will suggest four central points as criteria for a suitable approach to privacy. First, a definition of privacy must acknowledge the *contextual* nature of privacy. Privacy is arguably always embedded in both a micro and a macro context. Second, privacy must be discussed as a *social phenomenon*, since this is the perspective adopted in this thesis. However, the 'social' should be viewed on many levels, as I will argue below.

Third, an understanding of privacy must consider it as a *dynamic phenomenon.* There needs to be some account of change processes relating to privacy, particularly regarding new technologies. An adequate account of privacy must consider the emergent and constantly changing aspects of the social world, that is, social processes as well as structures. Fourth, privacy must also be considered as an *experienced phenomenon* in addition to being an objective, observable phenomenon. The contention is that privacy cannot be described only by means of behavioural indicators or expert discourse but an understanding of privacy must take into account how it is perceived and experienced by ordinary individuals (Lobet-Maris et al., 2012, pp. 47–48). The conceptions of individuals need to be taken seriously as a counterbalance to academic conceptions, since they can reveal which aspects of privacy are in reality felt as important. At the same time, one must be careful to distinguish between the objective and subjective sides of privacy. The objective side refers to aspects of the social structure and the functions of privacy, for instance. The subjective side relates to the privacy as it is experienced and valued by individuals. The following sections will develop an understanding of privacy based on these criteria and the existing literature. This understanding of privacy will guide the analysis of images of the future in the empirical part of the thesis.

3.1 General Definitions and the Contextuality of Privacy

Theories of privacy can be divided into groups in several ways. I will briefly discuss general categorisations of definitions before making my own classification in the next section. Solove (2008, pp. 12–13) divides conceptions of privacy into six general types:

1. The right to be let alone
2. Limited access to the self
3. Secrecy
4. Control over personal information
5. Personhood
6. Intimacy

Solove criticises all of these conceptions as either too narrow, too broad or both. That is, they are too vague and include many aspects which should remain outside the concept of privacy or they are too specific and exclude important aspects of privacy (Solove, 2008, pp. 12–36). Nissenbaum, in turn, organises theories of privacy along three dimensions of difference. Firstly, theories are either normative or descriptive. Secondly, they are framed either in terms of access or in terms of control. Thirdly, the prescriptive power of theories is either in promoting other important values (functionalism) or in protecting a specific private realm (Nissenbaum, 2010, p. 67). Nissenbaum, like Solove, sees previous theories as inadequate and presents her own contextual integrity approach as a synthesis that includes many of the strengths of previous theories (Nissenbaum, 2010, pp. 71, 126). Solove's and Nissenbaum's own theories will be discussed in section 3.2.

Tavani distinguishes between four types of privacy definitions: privacy as non-intrusion involving one's physical space (physical privacy), privacy as non-interference involving one's choices (decisional privacy), privacy as non-intrusion involving one's thoughts and identity (mental privacy) and privacy as control over one's information or limiting access to it (informational privacy).[10] The first three are seen as problematic and inadequate because they exclude aspects of privacy and include issues which are not strictly speaking privacy issues. Therefore, Tavani's own focus is on informational privacy, where he distinguishes between restricted access theories and control theories and the synthesis of these in the restricted access/limited control theory (RALC). In the RALC theory, individuals are protected by access restrictions while also having limited control to manage their privacy (Tavani, 2008, pp. 135–144).

Christian Fuchs (2011, pp. 222–223) connects these approaches to privacy with Anthony Giddens's division into subjective and objective approaches within social theory. Fuchs's account is presented in Table 1. The theoretical distinction between subjective and objective theories is useful for my account of privacy. However, I would argue that agency and structure are in this case more suitable terms for the theoretical criteria than subjectivism and objectivism, because control is exercised by individual agency while restricted access is a structural condition within society.

[10] Tavani describes these types both as "four distinct kinds of privacy" and as "alternative views" and criticises the first three views as inadequate definitions (2008, pp. 135–138). Therefore, it is not entirely clear whether they are intended as alternative definitions of privacy or as different aspects of privacy. I assume here that they are described as alternative definitions of privacy.

Table 1 Typology of privacy theories according to Fuchs (2011, p. 224)

Theoretical criterion	***Approach***	***Description***
Subjectivism	Control	Privacy as individual control and self-determination of the access of others to one's private sphere
Objectivism	Restricted access	Privacy as the right or norm of restricting others' access to one's personal affairs
Subject/object dialectic	Restricted access/control	Privacy as process, in which action regulates and manages the conditions of the private sphere and can thereby enable the existence of a protective sphere that allows individuals to act in society

Such general typologies and approaches are useful as summaries, but they tend to conflate very different conceptions of privacy. For instance, treating theories as control and restricted access theories ignores or takes for granted the *functions* of the control or access restrictions. Arguably an explanatory theory of privacy should look beyond behavioural aspects into *why* control or restricted access is important in various contexts. The problem with the restricted access/limited control notion of privacy, in particular, is that it usually focuses narrowly on informational privacy, neglecting issues of physical or mental intrusion, for example. Its foundations are in computer and information ethics, which are crucial fields for privacy discussions, but the issue of privacy does not only concern computers and information networks.

More recent theories of privacy have attempted to move beyond the perceived problems of previous theories. The restricted access/control theory was already discussed as one synthesis of previous approaches. Fuchs's solution to conceptualising privacy, in turn, is to promote a normative socialist theory of privacy which provides privacy for exploited and powerless groups while exposing the wrongdoings of the powerful. Privacy, in this conception, is a "collective right of dominated and exploited groups" (Fuchs, 2011, p. 232). In other words, Fuchs promotes a differentiated form of privacy based on one's position within society. For Fuchs, whether privacy should be protected or not depends crucially on the interests at stake in the particular context. If the interest is in collecting consumer information for commercial purposes, there should be privacy protection, whereas if the interest is in revealing corporate misconduct or inequalities of wealth, there should be no privacy protection. These interests are, in turn, connected to social structure and the political economy. Fuchs's conception is valuable because it connects privacy to the wider social structure and emphasises that privacy is embedded in a social context. However, the overall assessment of Fuchs's conception of privacy hinges on whether one accepts his Marxist starting point. While raising important issues, in my view it is too normative and ideological to be useful as a scientific conception of privacy.

In addition to Fuchs's Marxist criticism, theories of privacy have faced two central criticisms: an overly simplistic and essentialist view of privacy and maintaining an overly rigid private/public divide. Schoeman claims that due to the contested nature of privacy, it should not be defined precisely. Instead, the "contexts in which it arises or is invoked as a concern" should be studied (1992, p. 11). Solove (2008, p. ix) agrees, arguing that there is "no overarching conception of privacy – it must be mapped like a terrain, by painstakingly studying the landscape." For Solove, the fundamental problem with current theories of privacy is that they seek the 'essence' of privacy, a common denominator that unites all aspects of privacy. In Solove's view, there is no such core of privacy and therefore the search for it is fruitless (2008, p. 38). Nissenbaum (2010, pp. 91, 140–145), in turn, criticises a strict private/public divide, whether it is between actors (individual/government), realms (personal/political) or information (private/public), arguing instead for studying what she terms context-relative informational norms.

It could be argued that these theorists try to widen the discussion on privacy and recognise privacy as a more complex, contextual and multi-faceted concept. Privacy is no longer seen as a question of private and public information or space or viewed in terms of a single crucial value to which it is linked. Instead, privacy encompasses many aspects in different contexts. The acknowledgment of the contextuality of privacy is thus one of the strengths of recent privacy theories. Solove moves the definition of privacy towards multiplicity. Solove views privacy as a pluralistic umbrella term which refers to "a web of interconnected yet distinct things". His conception draws on Wittgenstein's notion of family resemblances between concepts as well as philosophical pragmatism (Solove, 2008, pp. 42–49). There is no easily discoverable 'essence' of privacy that is the same in every situation, but rather privacy issues always need to be examined contextually (Solove, 2008, p. 40).

Solove suggests a definition of privacy centred on problems that the law should address. He identifies 16 different privacy problems grouped under four headings: information collection, information processing, information dissemination and invasions. Solove's taxonomy of privacy problems is presented in Figure 3. According to Solove, these problems are a result of conflicting activities when the activities of governments, businesses and people hinder the valuable activities of others. Another interesting point about Solove's conception of privacy is that privacy is viewed as something that is constructed by means of law and technology. It is not a "resource existing in the state of nature that the law must act to conserve." Solove's reasoning is the following: certain situations are experienced as problems, they are then framed as privacy problems and thus create a desire for privacy (2008, pp. 64–65, 74–76). For Solove, problems are logically prior to privacy: they create the need for privacy. Therefore, according to this view, it is fallacious to claim that previously there was a state of privacy which is now threatened. Instead, privacy is that which emerges as a result of laws and policies tackling practical problems. The implication is that privacy is a dynamic phenomenon which changes through human action as legislation is created.

Solove's discussion of privacy problems brings concreteness to the study of privacy by focusing on activities and problems rather seeing privacy only as a condition. Solove in effect argues that the issues that previous privacy definitions have identified are real, but the conceptions are mistaken in excluding many other issues. In reality, privacy problems contain all of the 16 types of problems, most but not all of which are connected to information. In addition, Solove usefully connects the privacy problems into a model where they occur at different points in the chain from data subject to data holders and beyond.

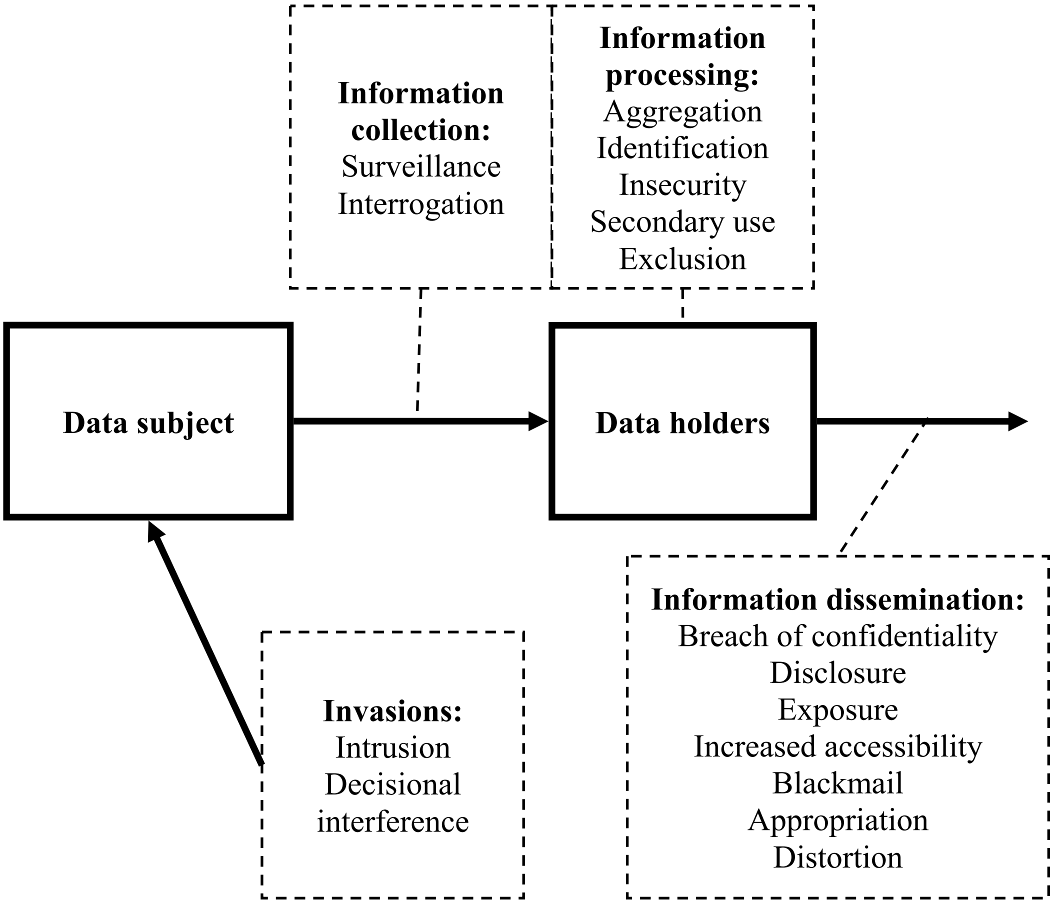

Figure 3 Taxonomy of privacy problems according to Solove (2008, p. 104)

Similarly, DeCew (1997, p. 61) promotes a conception of privacy as "a broad and multifaceted cluster concept" and argues for a 'reasonable person's' standard in assessing privacy claims. She outlines three separate but interrelated aspects of privacy: informational privacy, accessibility privacy and expressive privacy (1997, pp. 73–80). For DeCew, what unites these different privacy interests is that private matters are seen as beyond the legitimate concern of others *for certain reasons* to do with freedom from social pressures and judgment (1997, p. 66). In other words, similar functions unite different types of privacy. There is a clear overlap with Tavani's categorisation of four privacy definitions. The difference is that DeCew conflates physical and mental accessibility and prefers to write about expressive privacy rather than decisional privacy, although the decisions that are in question are largely self-expressive in nature and therefore the categories are very similar. Furthermore, while Tavani focuses on informational privacy as the most coherent definition, DeCew argues that a definition of privacy must include all types of privacy.

In this study, I agree with the inclusive definition because a narrow focus on information excludes other important aspects of privacy, as Solove's taxonomy of privacy violations demonstrates. Furthermore, including decisional and expressive aspects within the definition of privacy has the advantage of acknowledging that privacy is not only privacy *from* somebody but it is also privacy *for* something (Schoeman, 1992, p. 156). In other words, certain valuable ends are achieved by protecting privacy. The next sections will discuss the functions of privacy in more detail.

Recent privacy theories thus exhibit an awareness of the contextuality of privacy. However, to claim that privacy is contextual does not clarify the phenomenon very much. The contextuality of privacy must be explicated at various levels of society: concrete situations, social values and societal protection of privacy and so on. In the next section, I will explore these levels by focusing on the social aspects of privacy.

3.2 Privacy as a Social Phenomenon: A Categorisation of Privacy Theories

In the following, I will present my own categorisation of privacy theories which is used as a foundation for building my own approach to privacy. In the delimitations of the study, I limited the approach to privacy to its social dimension. However, the meaning of the 'social' should not be taken for granted. When privacy is viewed from the social perspective, it is still a rather complex phenomenon. Firstly, the 'social' involves many levels, from the microscopic level of individuals through the relational level of interaction and communication to the macroscopic level of societal privacy protection. From a critical realist perspective, macro phenomena should not be taken as given but instead there should be a discussion of how they emerge from the interaction of actors at the micro level (Elder-Vass, 2012, pp. 15–22; Hedström & Ylikoski, 2010, pp. 58–60).[11] Therefore, 'the social' seen as relational and emergent (Alvesson & Sköldberg, 2009, p. 43).

Secondly, privacy is an experienced, subjective phenomenon in addition to being an objective feature of interaction and society. According to the critical realist perspective adopted in this thesis, social reality has an existence outside subjective interpretations of it but it is produced by a large number of forces interacting in a complex way. There are also various interpretations of social reality by actors involved in it, and these interpretations are a part of the object of study as they are among the forces that influence behaviour. In other words, privacy can be analysed on many levels of social analysis, and both objective and subjective aspects of social reality need to be taken into account. George Ritzer's (2001) schematic of the major levels of social analysis is useful to distinguish between different aspects of privacy in a systematic way. Ritzer organises social analysis into four main levels along two continua: micro to macro and subjective to objective.[12] His general conception is illustrated below.

[11] On the other hand, social phenomena are the product of such long causal histories that their foundations are impossible to discover in practice. Therefore some macro phenomena must be taken as given in empirical research (Hedström & Swedberg, 1998, pp. 12–13). The problem of moving between micro and macro levels is, of course, a perennial topic of discussion which cannot be covered in depth in this thesis (cf. Rios, 2005).

[12] As Ritzer notes (2001, p. 99n), it is debatable whether subjective-objective should be seen as a continuum or a dichotomy, but it can be viewed as a split with mixed types in between. The micro/macro and subjective/objective divisions are similar to the quadrants of integral futures, where the dichotomies are individual/collective and inner/outer. However, the categories used in my study are arguably more suited to social scientific inquiry than Wilber's framework with its inclusion of spiritual knowledge (Slaughter, 2008; Voros, 2008, p. 198). The reservations about causal layered analysis that were discussed in section 2.3 also apply to integral futures.

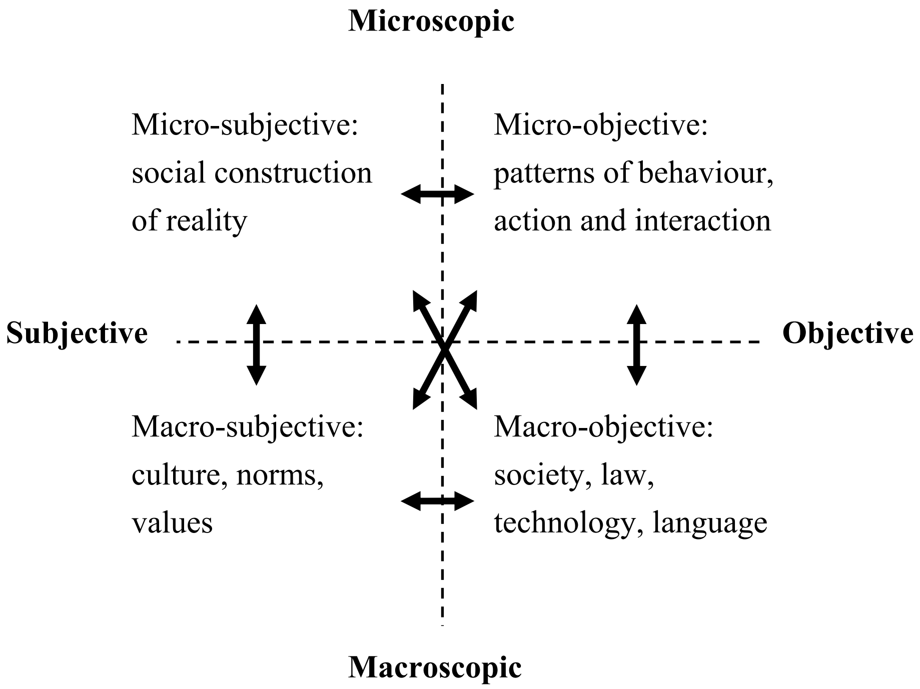
Microscopic
Micro-subjective: social construction of reality
Micro-objective: patterns of behaviour, action and interaction
Subjective
Objective
Macro-subjective: culture, norms, values
Macro-objective: society, law, technology, language
Macroscopic

Figure 4 Major levels of social analysis (Ritzer 2001, p. 93)

It is important to note that this division into two dimensions is an analytical tool and not an ontological feature of the social world as such (Ritzer, 2001, p. 81). The exact placing of language or norms, for instance, could be debated at length, but the central point is the inclusion of different levels into the analysis. The bidirectional arrows indicate that there are interconnections between all the levels. In addition, the whole image represents a snapshot at one point in time, and all the levels are subject to change processes.

Ritzer states that the issue under study should determine the choice of analytical approach and paradigm. He writes: “Not all sociological issues require an integrated approach, but it is certain that at least some do” (Ritzer, 2001, pp. 94–95). I would argue that in this study an integrated approach is beneficial for two reasons. Firstly, futures research in general requires an integrated approach because a narrow examination would risk neglecting important issues that crucially affect future developments. Issues in the past and present can be studied from a narrow disciplinary viewpoint, but studying futures and change processes arguably requires a holistic and systemic view. The role of the futurist is often as an integrator of knowledge produced by others, as Bell argues (Bell, 1997, pp. 90–92). Secondly, the issue of privacy in particular arguably also requires an integrated approach. The reasons for this have already been discussed above, but the main reason is that privacy does not fit comfortably in any conventional level or approach of social analysis. It is a phenomenon with important micro and macro dimensions as well as subjective and objective dimensions. There are thus two strong arguments for an integrated approach in this case.

My argument is that privacy has been conceptualised in various different ways mainly because theorists have focused on different explanatory levels on the micro-macro and subjective-objective continua. For classifying privacy theories, arguably three levels are needed on the micro-macro continuum: the individual, social relationships and society as a whole. All of these levels could also be analysed in terms of both subjective and objective theories, at least in theory. Table 2 illustrates how theories of privacy can be divided along these axes.

Table 2 Definitions of privacy

Level: micro to macro	***Subjective definitions: experiences, norms, values***	***Objective definitions: mechanisms, functions***
Individual	Privacy as control over personal information (Westin).	Privacy as a precondition for human dignity, respect for persons and moral autonomy (Bloustein, Benn, Reiman). Privacy as norms against overreaching social control (Schoeman). Privacy as the right to be let alone, limitation of access (Warren & Brandeis, Gavison).
Relational: Relationships and social groups	Privacy as contextual integrity. Maintaining context-relative informational norms which ensures that expectations about appropriate information flows are met (Nissenbaum).	Privacy as necessary for intimate relationships through differential sharing of personal information (Rachels, Fried). Privacy as a dynamic process of negotiating boundaries and maintaining self-identity in intersubjective relations (Steeves, Petronio). Privacy maintains the integrity of spheres of life (Schoeman).
Society	Privacy as a shared value (Regan).	Privacy as a feature of social structure that is constructed by norms and legislation (Solove). Privacy as a social mechanism operating at the boundaries of societal communication systems (Baghai).

Certainly the position of several theories in the table can be contested, but the central aim of the table is to demonstrate the complexity and dimensionality of privacy as a social phenomenon. The different levels shed light on why there has been no consensus on a definition of privacy. Privacy is difficult to define because it relates to many levels within society. In this sense, different conceptions of privacy can complement each other rather than being mutually exclusive. The conceptions of privacy will be discussed next before turning first to an assessment of the theories for the purposes of this study and then to the development of a preliminary model of privacy dynamics.

3.2.1 Individual-Subjective: Privacy as Control over Information

According to the influential definition put forward by Alan Westin (1967, p. 7), privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". There are four crucial elements in this brief definition. Firstly, privacy is seen as something which individuals, groups or institutions must actively claim and exercise. The claim aspect introduces the possibility of conflict into privacy issues. Secondly, privacy belongs not only to individuals but also groups and institutions, although his conception emphasises the individual aspects of privacy. Thirdly, privacy pertains to *information* which may be communicated to others. Fourthly, privacy means that individuals, groups or institutions *determine for themselves* the conditions of disclosure. In other words, privacy means *control* over information about oneself. Defining privacy as control over personal information is one of the predominant strands in theories of privacy (Solove, 2008, p. 24).

For Westin, there are four basic states of individual privacy: solitude, intimacy, anonymity and reserve. Solitude is described as the most complete privacy an individual can attain. Intimacy means a separation of a small unit such as a married couple from the wider society so that this unit can have a close relationship with frank communication. Anonymity refers to being unidentifiable while appearing in public or publishing ideas, and reserve refers to a "psychological barrier" or "mental distance" established to block intrusions (Westin, 1967, pp. 31–32). In Westin's view, privacy in social terms means "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means". Moreover, privacy is something which needs to be continually balanced with disclosure and communication (Westin, 1967, p. 7). On the whole, privacy is viewed from the individual's point of view, as control over personal information and as separation from the wider community. In accordance with liberal social thought, the needs of the individual and the needs of society are set against each other.

3.2.2 Individual-Objective: Moral Autonomy and Limited Access

The notion of privacy as separation from society is also clearly apparent in the limited access theories of privacy. The classic definition of the limited access theory of privacy is “the right be let alone” and the right to “inviolate personality” (Warren & Brandeis, 1890). Bloustein, Benn and Reiman promote normative conceptions of the functions of privacy rooted in human dignity and respect for persons and personhood. For Bloustein (1964/1984, pp. 163–165), personal dignity and integrity and the individual as a self-determining being are at stake in privacy violations. Benn similarly argues that privacy should be grounded in the principle of respect for persons as authentic subjects with their own projects and a consciousness of themselves as agents. From Benn’s perspective, respecting another individual’s privacy means treating them as a person whose projects may be affected by intrusions rather than as an object of scrutiny (1971/1984, pp. 228–229).

For Reiman, in turn, the context of caring gives meaning to the sharing of information. This context of caring is present in friendships and romantic relationships but not in the relationship with one’s therapist, for instance. Caring, then, gives weight to the information that is shared, regardless of the objective content of the information. Reiman agrees with Benn’s notion of respect for persons and argues that privacy is rooted in respect for personhood. For Reiman, “*Privacy is a social ritual by means of which an individual's moral title to his existence is conferred*” (emphasis in the original). Privacy is the mechanism by which a social group confers to its members their status as moral actors capable of shaping their own destiny. In Reiman’s view, privacy is involved in the original and continuing creation of persons out of human beings. Privacy, then, is a social practice or a social ritual which provides to people the moral ownership of their own thoughts and actions (Reiman, 1976/1984, pp. 305–310). Reiman’s view acts as a bridge between notions of privacy based on its meaning for individuals and for intimate relationships.

Ruth Gavison criticises these normative theories and argues that there needs to be a neutral, objective conception of privacy so that the level of privacy and changes in this level can be objectively examined prior to any moral judgment on the desirability of the situation. This neutral view of privacy depicts privacy as a situation of an individual vis-à-vis others or as a condition of life. For Gavison, privacy is limitation of access with three distinct components: limited information on an individual (secrecy), limited attention paid to an individual (anonymity) and limited physical access to an individual (solitude). The crucial difference with Westin’s control theory is that for Gavison, privacy is a condition which can in theory be measured, and it has to do with access and attention as well as information (1980/1984, pp. 349–351, 354).

Gavison lists several beneficial functions of privacy for individuals. These functions are providing the necessary context for essential activities, freedom from physical access (necessary for relaxation, learning and concentration), promotion of liberty of action, freedom from censure and ridicule, promotion of mental health, promotion of autonomy, promotion of human relations and limiting exposure, which enhances a sense of dignity (1980/1984, pp. 360–369). Gavison's treatment of the social functions of privacy, however, is much briefer and it refers to social functions gained indirectly through individual functions. She merely states that privacy encourages moral autonomy and may advance a more pluralistic, tolerant society, and that privacy is necessary for the functioning of the political system (e.g. private voting and private political associations and discussions) (1980/1984, pp. 369–370). For Gavison, privacy is largely a matter of the separation of individuals from society, but the means is limiting access rather than the control over information promoted by Westin.

Defining privacy as an objective condition of being more or less separate from society runs the risk of neglecting the processual and contextual nature of privacy. One important aspect of privacy is that it is negotiated in intersubjective interaction. Ferdinand Schoeman's theory acts as a bridge between theories rooted in the individual and in interaction by incorporating both individual and relational aspects. The individual dimension of Schoeman's conception of privacy is that he defines the function of privacy norms as the protection of individuals from the overreaching control of others, similar to the constitutional protection of individuals from legal coercion. For Schoeman, privacy norms are nuanced and informal ways of defending the individual against social coercion (1992, p. 22). It is probably due to this definition that Schoeman has been classified as a 'limited access' theorist (e.g. Fuchs, 2011, p. 223). This classification is generally justified but with two qualifications. Firstly, it must be noted that limited access for Schoeman is contextual rather a dichotomy of private and public: "It is relative to given people, in a given situation, within a given domain, and to a given capacity" (Schoeman, 1992, p. 165). Secondly, I would argue that Schoeman's notion of the integrity of spheres of life is as important as his notion of limited social scrutiny. This notion will be discussed in the next section after the classic texts on privacy as relational.

3.2.3 Relational-Objective: Intimacy, Interpersonal Boundaries and Spheres of Life

Many scholars have acknowledged that privacy is linked to interpersonal relations. In particular, privacy has been viewed as important for intimate relationships. For Charles Fried (1968/1984), privacy has an intrinsic value. Fried's view is rooted in Kant's imperative to treat other persons as ends in themselves and never purely as means to an end (Kant, 1785/2002, pp. 46–47). Fried frames privacy in the context of morality and fundamental relationships of respect, love, friendship and trust. Privacy is necessary for this kind of relationships, because it provides the “moral capital” for fostering intimacy by making possible the control over information which is shared. For Fried, privacy is control over information about oneself (1968/1984, pp. 205–211). James Rachels (1975/1984) advances a similar argument, claiming that privacy, as the ability to control who has access to us and to information about us, is necessary for maintaining various different kinds of relationships. According to Rachels, an important facet of a particular relationship is the appropriate amount and kind of information for the other to have. Maintaining a system of different relationships necessitates control over access to us and to information about us. Rachels argues that “a fact about ourselves is someone's business if there is a specific social relationship between us which entitles them to know” (1975/1984, pp. 292–297).

Fried and Rachels, like Westin before them, promote a conception of privacy centred on control. However, what is crucial about these later theories is that control is a means for forming and maintaining meaningful relationships rather than an end in itself or a means for the seclusion of individuals. Reiman (1976/1984) criticises what he terms the ‘Rachels-Fried thesis’ of privacy as moral capital regulating social relationships. According to Reiman, Rachels and Fried espouse a market notion of intimacy, that is, intimacy constituted by scarcity and exclusivity of information. Reiman argues that intimate relationships do not necessarily imply exclusivity and that sharing information does not automatically imply intimacy (1976/1984, pp. 304–305).

Valerie Steeves (2009, p. 193), drawing on social psychology and symbolic interactionism, argues that privacy is a “dynamic process of negotiating boundaries in intersubjective relations”. From this perspective, privacy is created and negotiated in social relationships, and privacy as a social fact emerges from these negotiation processes. The strength of this intersubjective view is that it roots privacy in interaction among people and views privacy as a dynamic process rather than a static condition. According to this view, the functions of privacy are the development and management of roles and development of self-identity, in addition to regulating interpersonal boundaries (Altman, quoted in Steeves, 2009, p. 202). By regulating interpersonal boundaries, privacy enables persons to develop their self-identity, their sense of who they are. This is similar to Benn’s and Reiman’s personhood arguments but rooted in the framework of social interaction. From the intersubjective perspective, surveillance is a particularly problematic practice because it denies the contextuality and role-dependency of an individual’s actions and removes the possibility of intersubjective negotiation (Steeves, 2009, pp. 205–206).

The theory of communication privacy management within the field of communication studies also utilises the metaphor of privacy as a boundary negotiation process. The theory also usefully acknowledges that privacy is often co-managed by a group which establishes its own rules to control access to shared private information. In this case, individuals have to negotiate a situation of multiple intersecting boundaries. However, the focus in communication privacy management is on the rules that individuals utilise for controlling disclosure of private information, and privacy is understood narrowly in terms of ownership of private information (Petronio, 2002, pp. 2–5, 20–21).

There is also a danger in boundary theories that focus on individual action: they may leave the individual with the responsibility of protecting privacy and ignore the importance of societal privacy protection (Steeves, 2009, p. 200). Communication privacy management examines privacy in a situation where individuals can exercise control over information and in that sense privacy is not an issue. While the theory clarifies how individuals exercise control over their information, it is arguably less useful for my purposes. For studying the futures of privacy, it is more important to study the functions and preconditions of privacy rather than how individuals exercise privacy. In addition, intersubjective theories may also exaggerate the negotiated and socially constructed nature of privacy and ignore social and political power and the limits of social construction.

For Schoeman, already discussed above, privacy is not only limited access and protection from overreaching social control, but it also connects to the possibility of forming meaningful relationships (Schoeman, 1992, p. 21). For Schoeman, "privacy is important largely because of how it facilitates association with people, not independence from people" (1992, p. 8). Schoeman develops Reiman's and Benn's theories of autonomy and personhood by acknowledging that humans develop in interaction with others and that this outside influence can be positive and constructive as well as negative. Privacy protects social freedom, "options among associative ties", rather than the isolated individual (1992, pp. 6–7). Schoeman argues that privacy helps to maintain the integrity of different spheres of life in a historical context where specialised associations have taken over some of the roles that the local community had in the past. Schoeman views life spheres as rule-bound associational ties that are both smaller and larger than the individual. They are smaller because individuals usually participate in many spheres, and they are larger because the spheres consist of more than one individual. The model of individuals as overlapping circles is thus apt. For Schoeman, meaning is located within these relationships and autonomy can be seen as a means to the end of forming relationships (1992, pp. 110, 157–159). In a sense, Schoeman synthesises previous theories which focused on autonomy and on personal relationships.

Schoeman's theory of privacy as integrity of spheres of life incorporates both objective and subjective aspects, but in my view the objective aspect is predominant because an important part of the theory is a functional explanation of how privacy actually operates within society. Privacy is seen as a kind of social mechanism which operates at the micro level of relationship-building. Through limiting access to persons within spheres of life, privacy enables building relationships and maintaining several separate spheres of life. The state, the society or any other central power cannot control individuals completely since individuals have several groups to which they can belong and which are private with relation to other groups. According to Schoeman, this is characteristic of contemporary Western societies due to historical processes such as the growth of the market economy and the rise of mobility which brought with them increasing individualism and a respect for human dignity (1992, pp. 129–134, 153).

Although Schoeman's account illuminates important aspects of privacy, it can be argued that it only takes one dimension of privacy into consideration: the freedom from social scrutiny that enables individuals to make autonomous decisions and maintain the integrity of spheres of life. As DeCew (1997, p. 73) points out, it is unclear how informational privacy, for instance, should be considered in Schoeman's terms.

3.2.4 Relational-Subjective: Contextual Integrity

Arguably Helen Nissenbaum's contextual integrity theory synthesises the traditional focus on information with Schoeman's focus on spheres of life. Nissenbaum argues for an approach to privacy centred on context-relative informational norms, claiming that this approach occupies a middle ground between concrete interest politics in a particular situation and abstract accounts based on universal human values (2010, pp. 3, 10). Nissenbaum thus explicitly situates her privacy theory between the micro level of individual situations and the macro level of shared values. Privacy is seen as linked to norms protecting the integrity of specific social contexts such as healthcare or education. These norms ensure the appropriate flow of information within a context so that people's expectations about appropriate flows of information are met (2010, p. 231). The right to privacy then becomes a right to have one's privacy expectations met.

For Nissenbaum, information flows always occur in a social context. She defines contexts as "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)" (2010, p. 132). Examples of contexts are healthcare, education, employment, family and the marketplace. Contexts can overlap and they can be nested within each other, such as grade school within education (2010, pp. 130, 136). Context-relative informational norms, in turn, have four key parameters: contexts, actors (as subjects, senders and recipients of information), attributes of the information and transmission principles (2010, pp. 140–145). From this perspective, the principle of control and limited access, discussed above, are only two possible transmission principles.

Contextual integrity acts as a benchmark for assessing privacy. It is “preserved when informational norms are respected and violated when informational norms are breached” (Nissenbaum, 2010, p. 140). Nissenbaum’s theory contextualises privacy and clarifies the complexity involved in privacy norms. Information with certain attributes is private within a certain context, it is private from certain actors but not others and certain transmission principles are acceptable. The focus on contextual norms and expectations of appropriate information flows can be seen as a contextual update of the ‘reasonable person’ standard of privacy expectations presented by DeCew, among others.

3.2.5 Societal-Subjective: Privacy as a Social Value

Nissenbaum’s theory builds on Priscilla Regan’s (1995) theory of the social value of privacy. Nevertheless, it is useful to summarise Regan’s argument here because the focus is broader than in Nissenbaum’s theory. Drawing on normative theory, Regan criticises the traditional liberal notion of privacy as the individual’s interest in withdrawing from society. She argues that privacy is a common, public and collective value in addition to supporting individual interests. Privacy is a common value because it is commonly shared as a commitment even though its meaning may vary for each individual. Privacy is a public value because it enables exercising democratic rights and restrains arbitrary government power. It also enables citizens to come together in the public realm, thus supporting the democratic political system. This is achieved by hiding the unique characteristics of individuals in the private realm so that they can focus on their commonalities in public life. Finally, privacy is a collective good, like clean air, because it is non-excludable and indivisible. In other words, for anyone to have privacy, everyone has to have privacy. Because privacy is a collective good rather than the private property of individuals, it is better protected by public regulation than by the market, according to Regan. Regan states three reasons for this: the interests of record holders, the non-voluntary nature of many record-keeping relationships and computer and telecommunications technologies (Regan, 1995, pp. 220–231).

In sum, according to Regan, privacy is important ”because individuals share common perceptions about the importance and meaning of privacy, because it serves as a restraint on how organizations use their power, and because privacy – or the lack of privacy – is built into systems and organizational practices and procedures” (1995, p. 23). However, Regan focuses more on the normative side of privacy and less on what privacy is and how it functions.

Regan's conception provides a counterbalance to two earlier types of privacy conceptions: liberal views where privacy is only viewed as functional for the individual and communitarian views where privacy is viewed as a right of individuals to be balanced with concerns for the common good. From the communitarian point of view, privacy benefits the individual at the cost of the community, while limiting privacy tends to have positive impacts for the community. For example, Etzioni (1999, pp. 12–13, 187–188) argues that privacy should be limited as little as possible and only as a last resort, but privacy should always be balanced with concerns for the common good such as public safety. There is a clear contrast with Regan's view which claims that privacy *is* an aspect of the common good rather than an interest of individuals.

Although Alan Westin's own privacy conception is focused on the individual, he has also traced the history of privacy as a social issue and a shared value in the United States. Westin recognises three main causes of privacy developments: new technologies and their applications; attitudes of the public; and organisational policies and law. According to Westin, in the years following World War II privacy was seen as a relatively unimportant issue, but the rise of information technology since the 1960s gave rise to privacy concerns and even alarmist comments. Since then, privacy rose to the status of a central issue, particularly during the 1990s due to developments in technologies such as the Internet, wireless communications, genetic technologies, data mining and consumer profiling. However, the terrorist attacks of September 11, 2001 changed the balance of attitudes in favour of security and surveillance (Westin, 2003, pp. 434–449). Westin's account could be extended to include the privacy advocacy that has followed the measures taken after the terrorist attacks. The history of privacy as a social issue supports Regan's notion of privacy as a common value.

3.2.6 Societal-Objective: Privacy as a Feature of Society

The societal-objective level is perhaps the most intuitive understanding of the social perspective on privacy. From this perspective, privacy is a Durkheimian social fact which exists as a feature of society independent from the perceptions of particular individuals (Durkheim, 1895/1964, pp. 1–13). Liberal privacy theories focusing on the conflict between the individual and society often neglect this perspective. Daniel Solove (2008, pp. 92–93), in contrast, argues for recognising the social value of privacy and states that privacy is not only a psychological need or desire, but "a profound dimension of social structure" and "constitutive of society" by protecting private life in order for people to participate in public life.

Furthermore, Solove argues that an understanding of privacy must be contextual and socially and historically situated. According to him, privacy is constructed by culturally and historically contingent norms, activities and legal protections, and therefore a theory of privacy needs to “work from within history and culture, not from a position outside” (2008, p. 41). Solove also explicitly states that privacy cannot be seen as individuals simply escaping from society: "Privacy is not just freedom from social control but is in fact a socially constructed form of protection" (2008, p. 174). In other words, privacy must be seen as a culturally, socially and historically conditioned and positioned phenomenon. Privacy should be discussed in a particular society at a particular time rather than positing a definition of privacy that applies to all contexts and at all times.

It was established above in section 3.1 that Solove views privacy as a phenomenon that is constructed through legislation which protects individuals from certain activities. Therefore, the macro-social phenomenon of privacy would be the aggregate of this protection against specific harms. Importantly, privacy harms are not only individual harms but they also have a societal dimension. Solove connects many privacy harms to power relations. For instance, methods of information collection and processing, such as surveillance and aggregation, increase the power that governments, corporations and other individuals have over individuals. They thus affect the allocation and balance of power on the societal level, enforce social norms and divest people of control over their own lives (Solove, 2008, pp. 107–135, 181). This notion is similar to Schoeman’s conception of overreaching social control. On the macro-societal level, Solove argues that privacy protection influences power and freedom within society through protecting valuable activities, and this is also where the social and individual value of privacy stems from (2008, p. 93).

Solove’s conception is useful because it does not deny the normative aspect of privacy but rather combines the normative and descriptive sides of privacy. According to Solove, privacy is valued in contemporary societies because these societies value the activities that it enables and the kinds of social structure and power relations that it promotes. Following Schoeman, it could be added that the valuable activities include forming relationships and taking part in various spheres of life free from a totalising societal influence and vulnerability to social control. There is also a clear connection to Regan’s notion of privacy as a public value which enables the formation of the public.

An explicitly societal theory of privacy is provided by Baghai (2012), who argues for a privacy conception rooted in Niklas Luhmann’s social systems theory (Luhmann, 2002/2013). The strength of Baghai’s conceptualisation is that it considers the connection of privacy to changes in societal structures, particularly the differentiation of social contexts or worlds such as the economy, science and politics. Following Luhmann, Baghai views these social worlds as communicative systems which have their own selection criteria regarding which communication belongs to these systems and which does not. For Baghai, the general selection criterion for whether some communication is considered private or public is its functional relevance for a particular system (2012, pp.

953–958). Therefore, privacy conflicts “arise when an event in one social system becomes relevant, arguably without justification, to selection of communication in another system” (2012, p. 956). Privacy is then a kind of social mechanism operating at the boundaries of societal communication systems. According to Baghai, privacy enables societal communication systems to be loosely compatible with each other (2012, p. 958). The risk of privacy violations is augmented by the increasing complexity of social communication because it is increasingly difficult to place communication unequivocally in one social world or another.

It is then clear that Baghai considers privacy as a very different phenomenon than Solove, who views it as protections constructed against particular violations. For Baghai, privacy is instead linked to functional needs of the social system and as such it is arguably something that emerges rather than something that is constructed. Baghai’s theory shares much with Nissenbaum’s contextual integrity, but the former connects the functions of privacy to societal changes on the macro level.

A theory that is influential in information ethics is Floridi’s ontological interpretation of privacy. Floridi’s theory is difficult to fit into any of the levels of analysis presented here because it reconceptualises the social world in such a radical way. For Floridi, current conceptions of privacy belong to an old industrial culture. He argues that digitalisation and informationalisation have led to an ontological shift as a result of which personal information constitutes individuals. Since individuals increasingly *are* their information, violation of informational privacy is more akin to kidnapping than trespass or theft (Floridi, 2005). From Floridi’s perspective, informational, psychological and physical privacy effectively become the same thing because they all relate to information in the contemporary world.

While Floridi’s point of view is innovative and interesting from the perspective of futures research and I agree with him about the importance of digital ICTs, I find his ontological framework difficult to accept. In my view, giving up the view of humans as physical, material beings distinguishable from purely informational beings risks missing many important privacy issues in the material world. Even today, privacy does not only concern the cyber world of online networks but also the material world – one’s home and one’s body in addition to one’s online presence. On the issue of the rise of digital ICTs, I would argue for a more traditional interpretation that the importance of informational privacy is in fact rising in comparison with accessibility privacy and expressive privacy, but this does not mean that all of these dimensions can be reduced to informational privacy.

3.3 Towards an Integrated View

3.3.1 Assessment of Privacy Theories

It is clear that all of the privacy theories discussed above cannot be simply synthesised. However, I will suggest here a preliminary conceptualisation of privacy that will take into account many of the strengths of previous theories. I will first critically assess some of the theories from the perspective of this study and then develop a preliminary conceptualisation to be used in this study. The main theoretical contributions to my own view are from Solove, Nissenbaum, Schoeman and DeCew. As was already mentioned, for this study, a theory of privacy must take into account four crucial aspects: the contextuality of privacy, the social nature of privacy at different levels, the dynamic nature of privacy and privacy as an experienced phenomenon. The challenge is to find a conception of privacy that will allow the heterogeneity and multiplicity of phenomena that fall under it as well as taking into account the different societal levels.

Both Solove and Nissenbaum provide useful initial frameworks that try to overcome the perceived problems in previous privacy theories. Both theorists focus on concrete privacy issues that emerge in real contexts. For Solove, these are the privacy problems faced by data subjects, while for Nissenbaum they are new technological systems which challenge context-relative informational norms. Solove's framework is useful because it focuses explicitly on activities that may violate privacy. This relates privacy to something that social actors do rather than discussing privacy as an abstract condition within society. However, I prefer to use the closely related term *practices*, because it emphasises the notion that privacy-related activities are customary, patterned and systemic practices rather than isolated deeds.

On the other hand, there are some issues with Solove's approach that make it unsuitable for my purposes. Solove's research interest is primarily instrumental. He explicitly states that facilitating the crafting of legal and policy solutions to problem is a central aim of theorising about privacy (2008, p. 39). Correspondingly, Solove's research approach is pragmatic: building a privacy theory from the bottom up, starting with concrete privacy harms. Solove's view of privacy as an umbrella term with family resemblances as well as his taxonomy of privacy problems can be seen as micro-level theorising on a rather low level of abstraction. Solove explicitly considers his work as building a theory of privacy from the bottom up, as specific protections against specific related problems (2008, p. 40). The theory focuses on problems that are viewed as privacy problems in ordinary language and there are no theoretical criteria for explaining why they are framed as privacy problems. Solove is also relativistic regarding the kinds of activities that are regarded as valuable and are disrupted by privacy violations.

In addition, this pragmatic approach does not fit a critical realist starting point which aims at finding the real causal processes behind ways of discussing phenomena in language (Hedström & Ylikoski, 2010, p. 64). Usage of the word ‘privacy’ in ordinary language can be a starting point for theory, but I would argue that for studying the futures of privacy, a middle-range theory is needed to explain particular instances of privacy violations. I agree with Solove (2008, p. 40) that “privacy issues should be worked out contextually rather than in the abstract”. However, in my view, the context should be viewed more broadly instead of listing particular privacy violations.

Nissenbaum’s approach supplements Solove’s treatment of privacy-violating practices with a focus on contextual norms concerning the appropriate flow of information. The focus on norms is beneficial in two ways. Firstly, it places privacy in the social world rather than the abstract world of values. Secondly, norms are unobservable analytical constructs which help to explain why and how privacy violations are experienced rather than simply listing and describing such violations (Hedström & Swedberg, 1998, p. 13). In other words, they provide hints of the mechanisms behind how privacy is perceived in different situations. Nissenbaum’s discussion of the parameters of norms (contexts, actors, attributes and transmission principles) clarifies the contextual features of norms. Overall, the focus on norms provides a suitable middle-range abstraction for dealing with privacy harms.

However, from the perspective of this study, Nissenbaum’s contextual integrity approach has drawbacks related to three things: the focus on information flows, the agency of humans and the stability and objectivity of contexts. Firstly, the informational focus ignores privacy violations, such as intrusions into one’s home, which are related to access and do not concern information. The focus on information flows in contexts also downplays the role of human agency and interaction and makes technological systems the primary actor. Bellanova notes that Nissenbaum shifts the protection of privacy from the protection of individuals to the protection of institutionalised contexts, and external socio-technical systems are seen as the only threats to the consensus within contexts. Thus technology is the only actor that causes social change (Bellanova, 2011, p. 394).

Moreover, while technological systems are seen to change norms, the theory takes contextual values, the ultimate aims of a particular context, as given (Nissenbaum, 2010, p. 180). As a result, contexts are seen as rather static and harmonious entities. Nissenbaum acknowledges that contexts change over history and that they include power structures (2010, pp. 132, 135). However, little attention is paid to the mechanisms through which contexts are actively formed and maintained by human interaction.

An alternative view of social life would emphasise fluidity, conflicts and continuous negotiation regarding contexts and their norms and values. Many actors with different roles and potentially conflicting interests engage in this negotiation. An example of this is companies that introduce new employee surveillance systems to increase employee efficiency. The company is then trying to change the privacy norms of the workplace by introducing a new technological system, and the employer may have much more power than the employees to affect the situation. Another example is the discussion on the aims of the higher education system where there are many positions endorsed by different actors: higher education as a part of the national innovation system, as a provider of competent workers and as a provider of a broad education to citizens, for instance. The contextual integrity theory can thus be criticised for downplaying the role of politics, power and the interests of actors in maintaining and negotiating contexts. A focus on stable contextual norms ignores constitutive struggles and power relations within contexts and political and economic power which can operate across multiple contexts (Bellanova, 2011, p. 394; Dawes, 2011, p. 122).

If the ultimate values of contexts are taken as given, there is a conservative assumption that the status quo is a valid starting point in considering privacy. The current goals of the contexts are the only criteria for assessing the suitability of norms. From a futures point of view, it is problematic that there are no other criteria for deciding which contexts, norms and values could, in theory, be preferable to the current situation. Nissenbaum explicitly excludes a discussion of ultimate values from her analysis, concentrating instead social norms in contexts whose values are taken as given (2010, pp. 3, 10). Nissenbaum's perspective clashes with the notion of visions and images of the future as important drivers of social change, since in the theory existing contexts define which technologies and practices are acceptable.

Nissenbaum's theory also deals primarily with situations where norms favour privacy protection and new technologies challenge it. What about situations where social norms drift in the direction of lower privacy due to market pressures, for instance? Do individuals then have little grounds for claiming their privacy, if the low privacy norms efficiently serve the aims of socially valued contexts such as the market economy? The focus on the integrity of contextual norms can be problematic in such cases.

Baghai's account of privacy existing at the intersections of societal communication systems is open to similar criticisms than the ones aimed at Nissenbaum's contextual integrity theory. Both theories play down the role of actors and action by focusing on communication or flows of information. Especially Baghai's account in terms of functional communication systems nearly eliminates individuals and other actors from the social scene altogether, which in my view is unacceptable. The language of functional relevancy eliminates any potential disagreements or conflicts over definitions.

There are many similarities between Nissenbaum's and Schoeman's conceptions of privacy and in my view it is useful to compare them. Schoeman also focuses on norms and views privacy as a "system of nuanced social norms" which "modulates the effectiveness of social control over an individual" (1992, p. 6). Nissenbaum views privacy as related to the integrity of contexts while Schoeman focuses on the integrity of spheres of life. What are the differences between the approaches?

I would argue that there are two central differences. Firstly, Nissenbaum focuses on the subjective level of contextual norms, whereas Schoeman focuses on privacy as a kind of objectively existing social mechanism. Therefore, Schoeman can focus on the role of privacy in the *formation and maintenance* of spheres of life rather than taking these spheres or contexts as given. Arguably the spheres are seen as more dynamic and processual in Schoeman's thinking. For Schoeman, limited access to individuals by social scrutiny enables the formation and integrity of social spheres and ultimately the preservation of social freedom. This is linked to the second major difference, which is that Schoeman focuses on relations between individuals, that is, social relations, while Nissenbaum is focused on flows of information. This may seem like a trivial difference but I would argue that it is a very different focus. If one focuses on appropriate flows of information between actors, arguably there is the risk of objectifying the approach to privacy and losing sight of the interests of stakeholders. It could be argued that the function of flows of information is to create, maintain and modify relations between people. Therefore, the focus on social relations rather than information flows enables a discussion of power relations within society.

Nissenbaum acknowledges that her theory does not discuss possible conflicts between and among contexts and possible cross-cutting principles such as control over personal information (2010, pp. 239–241). In contrast, Schoeman's and Baghai's accounts help to understand that the intersectionality of contexts is precisely the situation where privacy has a role, although Schoeman's life spheres and Baghai's societal communication system are different kinds of theoretical constructs. Schoeman's and Baghai's accounts also help to understand the historical and macro-sociological background of privacy. Both authors view privacy as emerging from the differentiation of society into many spheres (Baghai, 2012, pp. 953–958; Schoeman, 1992, p. 110).

In addition to these main theories, some other theorists have also presented insights which need to be taken into account in a comprehensive theory of privacy. DeCew's typology of privacy helps by explicitly broadening the focus from only information to three crucial aspects of privacy: information, access and self-expression. Westin's differentiation between different ways of achieving privacy is also useful. From the individual's point of view, privacy can be divided into solitude, intimacy, anonymity and reserve. This categorisation clarifies that there are levels of privacy, not only a dichotomy of private and public.

Privacy, then, is related to informational and access norms in contexts or spheres of life as well as self-expression and freedom from social control. There is one more question to be discussed before moving to my own conceptualisation of privacy. What kind of phenomenon is privacy? Does it emerge in social interaction as a social fact or is it consciously constructed? For Solove, privacy is constructed by legislation, while theorists focusing on norms, values and interaction view privacy as a phenomenon that emerges in social interaction as individuals and groups actively protect their privacy. However, this apparent contradiction can be solved by acknowledging that privacy *norms* are emergent and privacy *laws* are written and codified versions of these norms. Norms and laws together provide the framework for privacy protection. Privacy protection thus incorporates both emergent and constructed aspects. I would argue that privacy-related norms are primary because they explain why privacy is seen as valuable and therefore why legislation is deemed necessary.

3.3.2 Privacy as an Institution for Maintaining Boundaries between Normative Circles

In contrast to theorists who maintain that privacy is inherently plural and indeterminate, I would argue that a definition of privacy can be formulated which takes into account the multiplicity of the phenomenon. The purpose of such a definition is to describe the *form* of privacy, separated from the content that the concept has in various circumstances. In my view, the most convincing theories of privacy are those that relate privacy to *boundaries* between entities and the *integrity* of entities. Privacy is viewed as a boundary between individuals, between social groups, between contexts or between societal communication systems. At the same time, privacy has to do with the integrity of these entities: the dignity, personhood and self-identity of the individual and the integrity of spheres of life, contexts or communication systems. The boundary metaphor is clearly an apt one for privacy.

At a high level of abstraction, privacy then has a homologous form at different levels. Following the liberal tradition, privacy is often characterised as a boundary between the individual and society or between private and public, but it is arguably more suitable to view it as relating to the boundaries between individuals or between normative groups of individuals, although it is ultimately always experienced at the individual level (e.g. Regan, 1995, p. 23). Threats to privacy can emerge from larger entities such as organisations and governments, but the function of privacy relates to individuals.

If privacy is seen as a means of negotiating boundaries, what precisely are the entities whose boundaries are negotiated? Different entities are suggested by different theorists: individuals (Petronio, Steeves), contexts (Nissenbaum), spheres of life (Schoeman) and social communication systems (Baghai). Correspondingly, the identified mechanisms are different at different levels. For example, Schoeman focuses on interaction between individuals within spheres of life while Nissenbaum's focus is on information flows. When theorising privacy from a social perspective, the researcher must be explicit about which analytical level is discussed and about the shifts between analytical levels: micro and macro on the one hand and objective and subjective factors on the other. It was suggested earlier that theories of privacy differ partly because they focus on different analytical levels. An integrated theory of privacy should account for all levels and for the shifts between them. This thesis can only take some initial steps towards such an integrated view.

I would argue that Dave Elder-Vass's concept of norm circles is a suitably general concept for the discussion of privacy as a social phenomenon. It also has the advantage of being rooted in the interaction of individuals on the micro level. Elder-Vass defines a norm circle as "the group of people who are committed to endorsing and enforcing a particular norm" (2012, p. 22). Norm circles refer to adherents of one norm, while the more general term 'normative circle' refers to adherents of one norm or a set of related norms (Elder-Vass, 2010, p. 132). Elder-Vass utilises the concept of normative circles in his critical realist social ontology. In particular, it is relevant to seeking mechanisms which enable social structures to have causal power. According to Elder-Vass, normative circles are groups of individuals which exert normative pressure on other individuals. However, the effect of a normative circle on an individual is not direct. It is mediated through the encounters that the individual has with members of the circle and with the individual's imagined normative circle, that is, her mental image of the normative circle (2012, p. 26). Normative circles affect individual behaviour and create tendencies for certain types of action but they do not determine the action of individuals. Their effect depends on the internalisation of norms and on the beliefs and attitudes of individuals. Thus, as Elder-Vass argues, the actual behaviour of individuals is always a sum of many interacting tendencies (2012, pp. 27–28).

Examples of normative circles are family, healthcare, law enforcement and online shopping, or a group of friends or a closed Facebook group. Each of these normative circles may include smaller circles within them and they may in turn be part of larger circles. Normative circles include norms about many aspects of attitudes and behaviour, but crucially there are also norms regarding appropriate information flows within and between circles as well as mental and physical access to individuals within a circle.

My argument is that privacy relates to normative circles in two ways. Firstly, privacy can be seen as a cluster of norms, a normative circle of its own with people, groups and whole cultures that endorse it. Secondly, privacy can be seen a means of maintaining the boundaries of different norm circles when they overlap with each other, that is, when individuals are subject to different and potentially conflicting normative requirements. This is my interpretation of the theories of contextual integrity (Nissenbaum), the integrity of spheres of life (Schoeman) and the integrity of social communication systems (Baghai). Normative circles vary greatly in size and in how committed individuals feel towards them. Each of them usually includes more than one person but they do not engage that person completely, that is, they do not normatively determine every aspect of her life. In this sense, they are both smaller and larger than individuals.[13]

These two ways in which privacy relates to normative circles correspond with Regan's two conceptual aspects of the social value of privacy. Regan's argument about the common, public and collective value of privacy was presented above (p. 46). Privacy as a common value corresponds to privacy as a wide normative circle, as a cluster of norms shared widely within society. In addition, I would argue that privacy as a public value, privacy facilitating the formation of 'the public', corresponds to the argument about privacy maintaining the integrity of normative circles. Translating Regan's argument to the terms used here, privacy enables the formation and maintaining of a particular type of normative circle, that of 'the public'. This is because privacy keeps people's personal characteristics private so that individuals can focus on each other's commonalities in public life and maintain the imagined normative circle of 'the public'.[14]

In the contemporary world, individuals are influenced by many normative circles. They belong to many groups, not just their family, the local community or 'the public'. These normative circles overlap and through individuals they are in a sense in interaction with each other. Elder-Vass calls this normative intersectionality and makes the following argument:

> *Normative intersectionality appears to be widespread in the contemporary social world, and if this is so the normative influence of social structure can no longer be seen as the effect of a monolithic 'society'. Rather, it is the result of diverse endorsing and enforcing pressures produced by a patchwork of overlapping normative circles. And in such societies, skilled social performances depend on a complex practical consciousness of the diversity, relevance, and extent of the range of normative circles in an individual's environment. Goffman's analysis of the ways we alter our performances in front stage and back stage environments is just one example of how such consciousness operates. (Elder-Vass, 2012, pp. 28–29)*

[13] Schoeman writes: "The model of circles overlapping, where each circle represents a person, is apt here. It displays intersections involving both less and more than one circle. Value is located in these intersections" (1992, p. 158). Using this metaphor, norm circles would be the intersections of the individuals. However, if individuals are conceived as circles, the image quickly becomes very complex due to overlapping norm circles.

[14] Regan's third notion, privacy as a collective good, arguably relates more to changes in privacy and to privacy protection, and it is in this sense different from the two others.

Elder-Vass's argument echoes Schoeman's (1992, p. 110) argument that the diffusion of value across many spheres of life is characteristic of contemporary societies, basing it on a more explicit social ontology.

My argument is that the 'skilled social performances' to which Elder-Vass refers depend on privacy, understood not as seclusion but as a set of norms relating to contexts. Privacy, I would suggest, is a means of reducing the complexity of overlapping norm circles by fixing certain boundaries around contexts or normative circles. These boundaries are drawn by establishing norms relating to practices in two domains: information flows and access to individuals. Access in this context refers to both physical and mental access. It includes the limitations on access and social scrutiny that Gavison and Schoeman write about. Many privacy norms are protected by mutual respect, trust and informal sanctions, but some of them are also codified in legislation. This boundary mechanism makes it easier for individuals to function in a complex social setting with conflicting normative demands. It clarifies the expectations that individuals may legitimately have regarding access and information flow in particular situations. Using a visual metaphor, it gives the social world clearer contours.

According to Solove, privacy violations occur when valuable activities of individuals and groups are disrupted by other activities such as surveillance. Solove takes the value of activities as a given, exogenous factor. For my model of privacy as boundary between norm circles, privacy violations do not need to disrupt activities that are particularly valuable. It is enough that the norm circle's norms regarding information flow and access to individuals are violated. Privacy can be said to be objectively violated when norms are broken even if the individual is unaware of this, for example when personal information is sold to third parties without consent. The individual experience of privacy violation, in turn, occurs when the internalised norms of individuals, again relating to a norm circle, are violated.

However, privacy norms protect particular kinds of valuable activity: freedom of association and the formation and maintenance of self-identity. I would suggest that information and access norms have emerged to protect the boundaries and integrity of normative circles and ultimately the social freedom of individuals, to use Schoeman's term. Social freedom refers to a kind of autonomy that does not mean immunity from social influence but options among associative ties (Schoeman, 1992, p. 7). In this sense, autonomy means determining one's self-identity and making one's decisions in interaction with various others rather than self-determination in isolation. It also means freedom from total control exercised by a single authority. From this perspective, individuals are free when they are not fully accountable for all their thoughts and actions to any normative circle. Certain contexts, such as one's home in many countries, of course have very strict privacy norms, sometimes even mandating solitude and the right to be let alone.

The link between privacy and social freedom (or autonomy or personhood) is thus *mediated* by the information and access norms pertaining to normative circles. These norms are means to the end of developing and maintaining the identity and integrity of norm circles and ultimately the social freedom of individuals. The underlying assumption is that normative circles are essential for the formation of the self-identity of individuals. They act as reference groups in the creation of social identity. Therefore, the theories emphasising respect, personhood and moral autonomy also grasp one important aspect of privacy. Individual dignity is preserved by maintaining the individual's ability to participate in many normative circles. In theory, a single individual can form a normative circle, if her opinions are very different from those of the surrounding society and she has formed them independently. This would be a case of true autonomy. However, I would agree with Schoeman (1992, pp. 5–7) that in real life this is an unrealistic case.

Therefore, the working definition of privacy in this study is the following: *Privacy is a social institution that consists of norms that govern practices involving information flow and access to individuals within normative circles.*[15] *These norms generally pertain to a particular normative circle but there may also be widely shared privacy norms. Privacy has three main functions. Firstly, it supports creating, maintaining and negotiating the boundaries of normative circles at different levels in the context of normative intersectionality. Secondly, by maintaining boundaries, privacy helps to develop and maintain the integrity, identity and differentiation of individuals and of normative circles. Thirdly, privacy reduces the complexity of interaction by limiting possibilities of action and clarifying normative expectations.*[16]

This is a description of the form of privacy separated from its content in particular cases. Understood in this sense, privacy consists of a group of contextual information and access norms which are grouped under the title of privacy. However, it is also more than a heap of norms. It is an institution which affects people's expectations and behaviour. This is because privacy norms are not only a cluster but they are related to each other by their similar form and functional purpose. In my view, the normative power of privacy comes from its function of maintaining boundaries and thus enabling individuals' social freedom and maintenance of self-identity. Contexts are thus protected not for themselves but in order to protect the social freedom of individuals.

[15] A brief definition of an institution is "the fixing of stereotyped social interactions in the form of rules" (Henning, 2007). An institution is here understood as a normative circle which is capable of influencing the behaviour of individuals.

[16] The argument that institutions reduce complexity was originally made by Arnold Gehlen (Henning, 2007).

A crucial aspect of this conception is that for privacy to protect the integrity of a normative circle, information and access norms must be followed by actors outside the normative circle. Therefore privacy norms arguably must constitute a wide normative circle that includes context-relative privacy norms. That is, context-relative norms regarding information flow and access must be widely shared within society. This can be seen as a paradoxical situation: a wide normative circle must support its own fragmentation into smaller circles. This paradox will be discussed in the empirical section.

This conception of privacy takes into account the historically changing and culturally relative nature of privacy. Particular normative circles will be different in different cultures but there are normative circles in all cultures and in all historical periods. The general concept of normative circle covers groups as different as a fly fishing club and the Islamic Ummah.

Moreover, the boundaries between norm circles are not static but they are in a constant process of negotiation where interests and power relations have a role. For instance, companies may try to spread the norms of commercial transactions into the healthcare context or the government may try to apply the norms of public administration into the higher education context. Privacy advocates may in turn try to push for stricter privacy norms and legislation. In addition, the norm circles themselves are not necessarily stable since their renewal depends on whether individuals and groups act according to norms. Similarly, the maintenance of privacy as an institution ultimately depends on whether individuals, companies and governments are committed to following privacy norms. Current privacy norms are not the only possible ones and not necessarily the best ones. This leaves space for imagining alternative futures with more desirable privacy norms and legislation. From the perspective presented here, norms are better if they better support the social freedom of individuals.

However, this very general conceptualisation of privacy is only preliminary and it leaves many questions open. For instance, how to account for different kinds of normative circles? It is plausible that individuals draw on their family and on groups such as sports clubs and musical subcultures for their identity. On the other hand, it is less plausible that individuals form their identities by visiting the dentist or the tax authority, which are normative circles in their own right. A preliminary argument could be that the context of caring that is central in Reiman's privacy theory is important here. Individuals form their identity and their social freedom based on relationships and groups that have meaning for them and to which they are committed. Privacy is clearly important in these contexts. On the other hand, privacy is also important in institutional contexts such as schooling and healthcare. This is clear from the fact that there is specific legislation in many countries concerning such contexts.

Another way of making the distinction between these two types of normative circles would be to say that the first intimate type has expressive functions while the second organised one has practical functions. A hypothesis could then be put forward that privacy is sought *from* certain more organised normative circles and it is sought *for* the individual and normative circles that are important for the individual. In each case, it is important to draw boundaries for the normative circles but for different reasons. However, what are the exact defining factors between these types of normative circles? It could be the context of caring and their meaning for individuals, but it could also be related to the size of the normative circle and to the strictness of norms and role requirements.

Another question is whether the privacy norms pertaining to normative circles are mostly similar or different across different circles. This has implications for legislation. If privacy norms are fundamentally similar, general legislation should protect privacy in many contexts. Comprehensive legislation would have the benefit of being more easily understandable for non-lawyers than complex sectoral legislation. However, if norms differ widely, a more sectoral approach is arguably preferable. Nissenbaum (2010, pp. 237–238) argues that since contexts differ, the sectoral approach of legislation within the United States is more suitable than the omnibus approach of the European Union. This is partly a normative question but it is also an empirical one. Subsequent studies should study contextual privacy norms empirically to determine whether they are similar or different.

These questions demand a more detailed analysis and cannot be answered within the space of this thesis. Therefore this definition of privacy must remain as a preliminary conceptualisation which may be questioned by subsequent research. However, the empirical part of this thesis does provide some support for its usefulness as a perspective.

3.4 The Dynamics of Privacy: Privacy as a Changing Phenomenon

The previous sections attempted to explain what kind of phenomenon privacy is and what functions it has in social life. For a discussion of the futures of privacy, a further understanding is needed of how privacy changes over time. This involves answering questions such as: What is it that changes when there is a change in privacy? What causes changes in privacy? In this section, I will outline a preliminary model of the dynamics of privacy and articulate the main elements and their interconnections. I will argue that like privacy, changes in privacy must be seen in terms of actors, interests and practices as well as the experiences and actions of individuals.

There are several complicating features in a discussion of privacy dynamics. First of all, what do we mean when we say that privacy changes? It was established above that privacy is an institution that consists of related norms with a similar functional purpose. Arguably, then, a change in privacy can mean at least three things. Firstly, it may mean that the norms relating to information flows and access change. This leads to an increase or decrease in the expectation and appreciation of privacy and to changes in behaviour. It could be argued that this change in itself is not problematic, if individuals are aware of what is happening and there is no conflict with their internalised norms. Secondly, a change in privacy may mean that privacy protection within society changes through new legislation, for instance. Thirdly, actual access to individuals and information flows may change due to new practices, which makes privacy norms practically impossible to uphold. The first two are non-material changes in norms and legislation, while the third type is a more visible change in actual social practices. These factors are of course interrelated: people tend to act according to norms and according to the law. In addition, in the long term, all of them are likely to change, probably in complex, interconnected ways. In all cases, problems emerge when the internalised norms and values of individuals are in conflict with one or more of these three: societal norms, societal privacy protection and actual social conditions. This leads to the experience of privacy violation rather than an acceptable loss of privacy.

In addition, it is important to differentiate between two types of changes in privacy. Firstly, privacy norms are part of a dynamic process where people interact among intersecting normative circles and normatively draw their boundaries. Therefore what is private and public within a particular context changes constantly, while the underlying nature of privacy itself stays the same. For example, much more information can be shared while the process of maintaining boundaries between normative circles remains the same. The second type of change is much more radical: it is possible that in the future the *structure* of privacy changes, that is, that it will mean something different than the boundary concept explicated here. This radical change can happen because of societal changes that change the structure of society as intersecting normative circles, for instance. Some of the emerging technologies discussed below may have a transformative effect on the role of privacy in society. However, it is assumed here that the general concept of privacy as normative boundaries between normative circles is likely to remain valid in the relatively near future.

From a philosophical point of view, there are objective and subjective components in the future of privacy. Firstly, there are the objective social conditions in which people live. There may be more or less possibilities for privacy in a society. One aspect of the future of privacy is the future of these social conditions. Secondly, the future of privacy involves the future of how privacy is perceived by people living under these conditions. These perceptions are influenced by various factors such as individual attitudes, socialisation and media debates. This is the difficult part in trying to examine possible futures. Not only can the future be radically different from today, it may also be experienced differently than how that same future would be experienced by people living today. Inayatullah (1999, p. 53) makes this point by claiming that real futures cause cognitive dissonance because we lack the epistemological frames to understand them. A phenomenon may cause concern now but it may be seen as less threatening in the future. Therefore it is difficult to assess at present whether changes in privacy norms are problematic or not. A future that is interpreted with the use of present categories is a *present future* as opposed to a *future present*, in the vocabulary of Adam and Groves (2007, pp. 196, 200).

On the other hand, interpretations can only be made using present categories unless one wishes to speculate about future understandings. The form and function of privacy as I interpret it, protecting normative circles and social freedom, is unlikely to change radically in the future. Therefore if social freedom is still valued in the future, privacy will also be a necessary means of protecting it. Furthermore, for a study of the futures of privacy from the social perspective, the preconditions of having privacy are more important than how privacy is actually exercised by individuals. In other words, it is more important to discuss whether individuals will continue to have possibilities for exercising privacy than it is to describe in detail how individuals choose to exercise it. From the perspective of social freedom, the objective conditions in the future are more important in images of the future than individuals' subjective perceptions of privacy or their privacy-related behaviour.

3.4.1 Outline of a Model of Privacy Dynamics

In accordance with the critical realist framework adopted in this study, changes in privacy must be seen from the perspective of actors, interaction and mechanisms. Actors with causal powers must be identified and there must be plausible mechanisms that produce observable changes. An outline of a model of privacy dynamics is presented below, followed by a discussion of its constituent parts. The model is presented for privacy violations where the subject is an individual rather than a group of individuals. There are two reasons for this. Firstly, in my view it is only reasonable to discuss internal features such as experience and internalised norms in the case of individuals. Secondly, the model considers individuals as members of groups, because privacy concerns individuals within a normative circle and the action that privacy protects is associating with others to maintain social freedom.

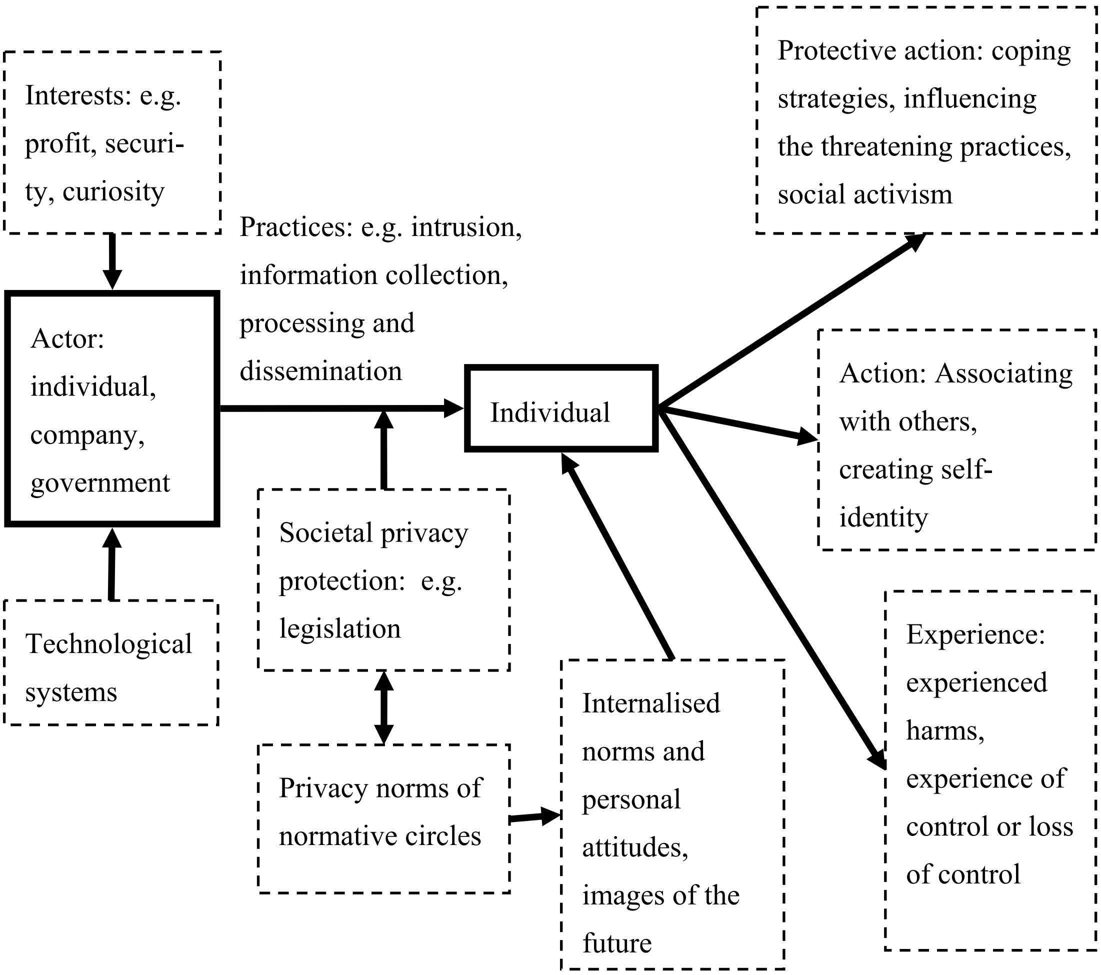
Interests: e.g. profit, security, curiosity
Actor: individual, company, government
Technological systems
Practices: e.g. intrusion, information collection, processing and dissemination
Individual
Societal privacy protection: e.g. legislation
Privacy norms of normative circles
Internalised norms and personal attitudes, images of the future
Protective action: coping strategies, influencing the threatening practices, social activism
Action: Associating with others, creating self-identity
Experience: experienced harms, experience of control or loss of control

Figure 5 Privacy dynamics model

In the figure, the solid boxes represent real actors and the boxes with dotted lines represent abstract features which relate to the situation through some mechanism. The model represents a particular situation facing an individual, since it is my contention that privacy is always experienced in a particular context and that, following Solove, privacy threats emerge from particular practices. Crucially, there are many dynamic elements within the model: interests, technologies, norms and legislation. All of these elements may change.

3.4.2 The Threat: Actors, Interests, Technologies and Practices

The link between new technologies and privacy threats has been posited countless times. There has been such an explosion of articles on the topic in recent years that a comprehensive literature review would be a large project in itself. The rise of digital information and communications technologies is often seen as the primary threat. Current privacy threats include tracking and monitoring technologies such as sensor networks and radio-frequency identification (RFID) tags, massive aggregated databases, 'big data' which can be mined for emerging patterns and online social networks such as popular social media sites (Lockton & Rosenberg, 2005; Nissenbaum, 2010, pt. 1). All of these technologies involve processing information, and indeed information has been identified as a crucial factor of production in the contemporary economy (Castells, 2000, Chapter 1; Drucker, 1993, pp. 42–43, 181).

In addition to information and communications technologies, several emerging technological fields can be added to the list of potential privacy threats. These fields include nanotechnology, biotechnology, cognitive technology and robotics. Moreover, the convergence of these technological fields is likely to present new threats (Brey, 2012; Hauptman & Katz, 2011, Chapter 3; Heinonen, 2001, 2011). There are many current technological advances and practices which could be seen as signals that anticipate radical transformations. Such technologies and practices include ubiquitous computing (or ambient intelligence), the Semantic Web, the Internet of Things, Google Glass and the quantified self or self-tracking (Arthur, 2013; Economist, 2012; Hert et al., 2008; Mannermaa, 2007; "Semantic Web - W3C," 2013; R. H. Weber, 2010). In many cases, whether potential social transformations are seen as beneficial or threatening depends on one's perspective.

The privacy dynamics model is an attempt to explore the more general dynamics behind these complex developments. Due to the high level of abstraction, specific technologies cannot be dealt with in detail in this thesis. From the social perspective, the privacy challenge of new technologies can be framed as a question of expectations based on social norms. Nissenbaum (2010, p. 231) argues that new digital technologies have introduced a discontinuity which puts privacy experiences and expectations at odds with each other. Floridi (2005) agrees that digital technologies are radically changing the social world and this has profound implications for privacy. The world is changing in a way that causes a kind of cognitive dissonance in individuals. For the purposes of this section, it is not enough to claim that new technologies pose potential threats to privacy. The general *mechanism* through which technologies threaten to violate privacy must be explicated. I will argue that three elements must be in place for privacy-violating practices to occur: technology, actors and interests.

The issue of privacy threats posed by new technologies is not an invention of the 21st century. Arguably its history dates back to at least Warren and Brandeis's (1890) article on privacy in the 1890s. In general, concern over privacy has risen together with new technological possibilities which pose potential threats to privacy (Gavison, 1980/1984, pp. 375–376; Westin, 2003). There are of course many historical examples of technologies being put to use before their full social and environmental implications are understood. Technology is often seen as an autonomous force that causes social changes, both positive and negative. On the one hand, technological development improves welfare and productivity. On the other hand, it may threaten fundamental human values and, at worst, the existence of humankind, whether through warfare guided by artificial intelligence or through environmental collapse. However, I would argue that technology must be contextualised and seen as embedded in social relations rather than seeing technology as an independent variable. In particular, Nissenbaum's, Regan's and Gavison's arguments provide tools for this contextualisation in the discussion of technology and privacy.

In Nissenbaum's contextual integrity theory, technological systems are seen as embedded in normative social contexts rather than existing as things separated from human beings. In order to function as technologies, systems such as telephones require complex networks of technical standards, policies and social norms. Therefore, privacy protection does not protect from particular technologies as such but it protects from technologies as they function in contexts and violate contextual norms (Nissenbaum, 2010, pp. 5, 184, 200). Technology is thus dangerous if it is used in practices that threaten the integrity of contexts and ultimately, I would add, the social freedom of individuals.

The role of technology in privacy dynamics is related to the more general question of the role of technology in social change which of course cannot be discussed at length here. According to Regan, on this topic thinkers can be divided into three schools of thought: technology determinists, technology neutralists and technology realists. In brief, determinists view technology as an end in itself and an autonomous causal agent which ultimately cannot be controlled.[17] Technology neutralists take the opposite view that technology is a tool which humans control and decide the ends to which it is put. Technology realists, in turn, try to synthesise between these extreme views. Technology is seen as a force but it is not independent of social and political forces. Technology sets certain limits and conditions but technology is in turn conditioned by social forces and decisions. According to this view, technology and society exist in a dynamic relationship where neither can ultimately determine the other. In addition, all the consequences of technological changes cannot be anticipated (Regan, 1995, pp. 11–13). Moreover, as Regan (1995, p. 68) argues, technology can be seen as an intervening factor which influences ideas and interests.

The view taken in this thesis is that of the technology realists, although both technological determinism and neutralism may be represented in the focus group discussions and they may form part of images of the future. Technologies by themselves are neutral in the sense that in theory, all technologies can be put into many different uses, both

[17] Some of the thinking on technological singularity can be seen to belong in this school of thought.

beneficent and malicious. However, in practice it is reasonable to say that technological systems give more affordances, that is, more action possibilities, for certain practices than others, and therefore they may bias the development of privacy-related practices. For instance, the development of massive networked databases is asymmetrical in the sense that once some piece of information has entered the database it is practically impossible to delete it permanently. It is difficult to see how massive databases could lend themselves to practices that increase privacy. Other technologies, such as cryptography, may give more affordances to privacy protection than privacy violation. Therefore it is fair to say that on the whole, new digital technologies can increase as well as decrease privacy, as Floridi (2005) argues.[18] However, this does not mean that each technology may increase or decrease privacy. Particular technologies may bias the development of privacy in either direction. There is no simple deterministic link between technology and changes in privacy.

Another important aspect of technology is that once a certain technology is introduced, it rarely completely disappears unless it is superseded by a more efficient technology used for the same ends. Once a technology is invented, it cannot be uninvented. Therefore technological and societal developments should be seen as path-dependent processes. Choices that were made in the past cannot be unmade or simply reversed, and there are significant lock-in effects with respect to technologies that are in use. In Adam and Groves's vocabulary, decisions have a certain *timeprint* that will affect the future in foreseeable and unforeseeable ways. The timeprint is a temporal equivalent of the footprint which relates to the future impacts of technological products (Adam & Groves, 2007, p. 105).

On the topic of privacy, it could be argued that no amount of potentially privacy-violating technology unequivocally makes privacy extinct. There is, however, a valid question whether protecting privacy becomes practically impossible or at least extremely costly in the new technological landscape, as Gavison suggests (1980/1984, p. 376). Froomkin (2000, p. 1465) also makes this point, arguing that quickly developing surveillance and data collection technologies may have transformative effects on modern life, making privacy impossible to attain in practice. Because technology can have such transformative effects, the development and application of technology involves power as well as responsibility (Heinonen, 2000, pp. 188–190). Furthermore, technological systems do not simply emerge but they are designed by actors for purposes which are also defined by some actors (Heinonen, 2001, p. 46).

[18] More precisely, Floridi's argument is that privacy does not simply increase or decrease due to digital ICTs but its meaning changes. As was stated above (p. 50), I will not adopt Floridi's radical ontological framework here.

It was argued above that technology is in a dynamic relationship with social forces. I would argue these social forces must be seen more specifically as actors, such as companies, governments or individuals, with particular interests. Interests are here used as an analytical tool and understood as driving forces behind the actions of actors.[19] In this context, interests should be seen broadly, encompassing not only economic self-interest but also political interests and other-regarding interests, for instance. Even simple curiosity can be seen as an interest that threatens privacy. Technologies, then, serve as tools for privacy invading-practices for those who wish to invade privacy for some reason. Therefore, new technologies create the *potential* for new privacy invasions by providing affordances to actors. From the point of view of the subject of the invasion, they create new *privacy risks*. Whether or not these risks are in fact realised depends, I would argue, on the *interests* at stake in the situation. Therefore, privacy-violating practices do not simply emerge, but they are implemented by particular actors, such as states and companies, with particular interests in establishing privacy-violating practices.

The notion of technologies united with interests is commonly made in the literature on privacy and technologies. Warren and Brandeis's classic article already mentions the "newspaper *enterprise*" and "[r]ecent inventions *and business methods*", suggesting that technologies in connection with commercial interests threaten privacy (1890, p. 195; emphasis added). It was mentioned above that Warren and Brandeis considered both technological inventions and business methods as posing a threat to privacy. Similarly, Regan (1995, p. 14) notes that in *Privacy and Freedom,* Alan Westin focused on the benefits that various actors gain through using privacy-violating technologies. Gavison also made a similar argument in the 1980s, stating that the privacy we enjoy is largely due to our anonymity and the fact that no-one is interested in us. Gavison writes: "What protects privacy is not the difficulty of invading it, but the lack of motive and interest of others to do so. The important point, however, is that if our privacy is invaded, it may be invaded today in more serious and more permanent ways than ever before" (1980/1984, p. 379). Due to new technologies, privacy is permanently in a fragile state. It can potentially be violated easily, if there is an interest to do so. It should be noted that the passage quoted above was written before the age of the internet, social media and widespread CCTV cameras.

[19] Definining 'interest' is not a simple matter because the concept is used in different ways by different theorists. Swedberg calls interest a 'proto-concept' and argues that "when it comes to the sociological concept of interest, everyone has to reinvent the wheel on her own" (Swedberg, 2005, p. 48). A more detailed account of the nature and role of interests would be beneficial but it cannot be attempted within the space of this thesis.

Even though interests have been brought up in the discussion, Regan (1995, pp. 218–220) argues that the interests of social organisations and issues of power imbalances have not been adequately examined in the literature on privacy. It is thus not enough to discuss the interests at stake in a particular situation but larger organised and patterned interests that are behind privacy-violating practices should also be studied. This also relates to the issue of control over personal information and access to oneself. Having control in theory means little if power relations make this control impossible to exercise in practice.

An alternative to the interest-based account would be to focus on conflicts between normative circles that enforce different norms. Privacy-violating practices can be seen as norms within certain norm circles: within governments, companies and among certain individuals, for instance. The concepts of norm and interest, understood as patterned and socially structured, are quite similar. However, the concept of interest emphasises the activity of agents and their striving for certain benefits for a limited group rather than acting in socially sanctioned ways. It can be argued that norms serve as means for actors to pursue their interests. In this sense, interests are primary to norms and they may influence changes in norms. For example, the interests of actors may drive them to push for changes in norms. Therefore the notion of interest is useful even though conflicting normative circles is also a valid description of the situation.

Ultimately threats to privacy posed by interests, technologies and practices should be studied empirically instead of merely making alarmist comments about the death of privacy. There may also be contexts where privacy norms are currently too strict, and efficient healthcare, for instance, could benefit from more free information flows. This thesis will focus on the subjective perceptions of threats to privacy that contribute to images of the future of individuals and the empirical material gives only indirect knowledge about real threats to privacy. However, this preliminary examination can give suggestions about where further studies could focus.

3.4.3 Norms and Legislation

Norms are at the centre of privacy protection, as the previous section argued. In the privacy dynamics model, privacy norms refer to those norms that concern flows of information within and across normative circles and access to individuals within normative circles. If the informational and access norms pertaining to a normative circle can be identified, they help to understand when privacy is violated. I would argue that objectively speaking, privacy is violated when practices affecting an individual within a normative circle conflict with the informational and access norms of that normative circle.

In the privacy dynamics model, societal privacy protection refers to legislation and other established means of collectively protecting privacy, such as the data protection authorities in Europe and the privacy commissioners in Australia, Canada and Hong Kong. This societal privacy protection has many tasks. In a simplified model it can be posited that their task is to influence the practices that potentially violate privacy by altering them so that they are less invasive or by outlawing them altogether. The clearest example is that a certain surveillance practice, such as surveillance of employees by their employer, is made illegal.

The bidirectional arrow between norms and societal privacy protection means that norms and societal privacy protection affect each other. Norms may become laws, laws may become norms and the two may sometimes be in conflict with each other (Bell, 2003, p. 118). It was suggested above that the normative value of privacy stems from its function as a boundary between individuals and between norm circles. However, interest groups may try to affect privacy norms and they certainly try to affect legislation. As I argued earlier, privacy is both emergent and constructed. Therefore legislation and norms are both potential driving forces that change the condition of privacy over time.

Clearly the societal norms and legislation around privacy are complex issues. For one thing, there are various laws, legal traditions and histories concerning privacy around the world. For example, a distinction is often made between the centralised approach taken in the European Union and the sectoral or contextual approach in the United States (Nissenbaum, 2010, p. 237; Solove, 2008, p. 185). In the United States, privacy protection has been seen as divided between tort privacy law and the constitutional right to privacy, while the Charter of Fundamental Rights of the European Union considers data protection as a separate right from the respect for private and family life (DeCew, 1997, p. 18; European Union, 2000). In addition, the creation and passing of legislation is a complex process involving what Regan (1995, p. 19) calls policy communities: researchers, interest groups and parliamentary staff, among others. The norms of particular normative circles are also difficult to identify and it is difficult to determine their spread and the extent to which individuals and other actors are committed to respecting them in behaviour. Due to these complexities, describing actual changes in legislation and norms is an enormous task and it will not be attempted in this thesis. The primary focus of this study is on the individual level where privacy is experienced, although subjective beliefs about the entire privacy dynamics model are also examined in the empirical section. The individual level will be discussed in the next section.

3.4.4 The Individual: Internalised Norms, Experience and Action

The final element in the model presented above is the individual who is the subject of the privacy-violating practices. Individuals are influenced by contextual norms through the process of norm internalisation. The norms pertaining to particular normative circles are internalised to a greater or lesser extent and the internalised norms are united with the individual's own attitudes, values and beliefs that have been formed by various means.

A complication relating to values, internalised norms and behaviour is that there may be a gap between professed values and actual behaviour. Empirical research on privacy within behavioural economics has demonstrated that people say they value privacy but in reality they tend to act inconsistently with this (Acquisti, 2009). Of course, this makes the treatment of internalised norms difficult. Can we say that there is an internalised norm when an individual claims to value privacy highly but does not usually act accordingly? On the one hand, norms create only tendencies of behaviour and they are resilient to exceptions. On the other hand, it is clearly inappropriate to speak of norms if the supposed norms are predominantly not followed. How many individuals must neglect a norm for it to cease to be a social norm? If norms are understood from Elder-Vass's critical realist perspective, as tendencies for a type of behaviour, norms are of course always in a process of change because they depend on new individuals committing to them. The value-action gap is a reminder that the situation is complex and that further empirical studies are required to understand how people actually behave in privacy-related matters. In this study, a rough understanding of norms as group-held beliefs about appropriate behaviour is sufficient. If they are increasingly challenged by practices or by lack of internalisation by individuals, we can speak of pressures for norm change.

There are two crucial aspects with relation to the individual: experience and action. The first one, experience, is influenced by the privacy-violating practices, on the one hand, and the individual's internalised norms and attitudes, on the other hand. A person's internalised norms and attitudes regarding privacy act as a kind of filter that determines whether certain practices are experienced as privacy violations. When there is a conflict between the practices and the internalised norms, there is an *experience* of privacy violation. This experience may coincide with an actual privacy violation when practices violate the privacy norms pertaining to a normative circle, but an objective violation of privacy and the experience of violation are conceptually separate. Inversely, there may be actual privacy violations which the individual does not experience as violations. This can happen for two reasons. Firstly, the individual's internalised norms and attitudes may not be in conflict with the practices. Secondly, the individual may be unaware of the practices, either because she has disregarded them or because the practices themselves are designed to be covert. In fact, one critical problem of privacy protection is covert surveillance and data processing, which is why it is important to make the distinction between experienced privacy violation and actual privacy violation.

Regarding action, there are three main types of protective actions that individuals can take when they experience privacy violations. Firstly, they can find ways of coping with the situation, for instance trying to change their attitudes or behaviour patterns in such a way that the privacy-violating practices do not bother them anymore. This type of action does not attempt to alter the privacy-violating practices themselves. Secondly, they can try to influence the particular practice which causes the privacy violation, for instance adding their name to a blacklist that prevents direct marketing from reaching them. This action can be seen as kind of local and pragmatic resistance. Thirdly, people can engage in social activism to promote privacy either as individuals or collectively. This kind of action constitutes more organised resistance and could potentially provide a feedback loop to the privacy-violating actors, their interests and the technological systems as well as to legislation. For example, if large numbers of consumers refused to use a company's products unless they change their privacy policies, it would be in the company's interest to reconsider its policies. Similarly, it is feasible that popular campaigning may affect privacy legislation or prevent the launch of a particular technology. However, the benefits gained from this approach are very uncertain and less direct than in the second approach.

The final dimension of individual action is the valuable activities which privacy protects: association with others and maintaining self-identity and social freedom. The function of privacy is to protect these activities, as the previous section argued. Therefore privacy-violating practices may risk these activities.

3.4.5 Societal Impacts Resulting from Loss of Privacy

Privacy-violating practices may have societal impacts in two ways. These could be called first-order and second-order impacts. Firstly, an overall threat to privacy emerges from privacy-related practices as they become common and patterned, for example in the case of pervasive surveillance. The overall impact may be larger than the parts taken separately, because if privacy violations become common, they may begin to affect the norms of normative circles through decision-makers and the actions of individuals. Small privacy violations may thus add up to much greater harms, and in a complex society with intersecting normative circles actions they may have impacts far beyond their immediate reach (Nissenbaum, 2010, pp. 241–243; Solove, 2008, pp. 177–178, 187). Because of this mechanism, even seemingly small privacy violations can contribute to an emerging threat to privacy. In addition, if privacy is seen as a collective good in

Regan's sense, a decrease in privacy for one individual will decrease it for everyone else, thus lowering the societal level of privacy.

Secondly, the diminishing of privacy is likely to cause further social impacts. If privacy is seen to regulate the boundaries of normative circles, loss of privacy would have impacts for both individuals and society as a whole. As was already noted above in the discussion of privacy theories, Solove argues that privacy violations cause a restructuring of societal power relations and the loss of control of individuals over their own lives. Normative circles could cease to be partly independent and be subsumed under a centralised normative circle such as the state or a powerful corporation – a kind of Big Brother – or perhaps there could be competing powerful organisations that would likewise exercise power over individuals and divest them of control. In any case, for individuals it would be likely to lead to fewer possibilities for defining their identities in relation to important normative circles and for freely associating with others in various normative circles. Individuals' control over their lives and their moral autonomy, understood as self-determination in relation to significant normative circles, would be diminished.

The contention that privacy violations and privacy protection affect the social allocation of power and the social structure has implications from a futures point of view. From this perspective, privacy protection does not only protect the interests of individuals but it is also connected to questions of what kind of society is desirable. Because privacy is a dynamic phenomenon with profound societal implications, it is important to study the possible and preferable futures of privacy. The next section will turn to the introduction of the material which will be used in examining images of the future of privacy.

4 RESEARCH MATERIAL: FOCUS GROUPS

The primary research material for the thesis consists of three focus group discussions which were held in three different countries: Finland, Germany and Israel. The focus groups were held in April and May 2012 as part of the PRACTIS project. PRACTIS (Privacy – Appraising Challenges to Technologies and Ethics) was a project funded by the European Commission's 7th Framework Programme for Research and Technological Development. The aims of the project were to investigate how emerging technologies may impact privacy and conceptions of privacy and to propose ethical and legal frameworks for dealing with privacy risks ("PRACTIS Project Objectives," 2010). The number of participants in the focus groups ranged from six to twelve, and in total there were 28 participants in the three focus groups. The participants answered four rounds of open questions and each round lasted approximately 30 minutes. The focus group questions are presented in Appendix 1: The Focus Group Questions. In the following, the features, benefits and potential problems of the focus group approach are discussed.

4.1 Why Focus Groups?

The choice of the focus group method was largely motivated by the availability of the material from the PRACTIS project, but there are also reasons why focus groups are a suitable data collection method for studying images of the future of privacy. According to Kitzinger (1995), focus groups are "a form of group interview that capitalises on communication between research participants in order to generate data". Communication and interaction are crucial characteristics of the method. The assumption is that by utilising group processes in the interview situation, people's knowledge and experiences can be examined in ways that would not be possible in one-to-one interviews. Within focus groups, participants can explore issues that are important to them using their own words and formulating their own questions. In addition to the views of single participants, focus groups can reveal shared understandings and explore differences of opinion in the actual discussion context (Kitzinger, 1995, unpaginated).

Focus groups are well suited to studying an issue such as privacy. As it was previously established, there is no widely shared definition of privacy. Therefore, it is important that participants are allowed to discuss privacy in their own vocabulary, exploring and revealing their own understandings of the topic. The focus group provides a forum for this discussion, although there is the danger that some participant's formulation of the issue may dominate over others. In any case, the topic of privacy is not set within a prior interpretive framework as would be the case in a questionnaire with closed questions. In this study, the focus groups are analysed with the aim of discovering different views, not with the aim of finding a consensus among all the participants. Nevertheless, these different views can be grouped into clusters according to certain criteria, as will be argued in the next chapter.

Table 3 presents the gender distribution of the focus group participants.

Table 3 Gender distribution of the focus group participants

	Male	*Female*	*Total*
Finland	5	5	10
Germany	4	2	6
Israel	8	4	12
Total	17	11	28

The table demonstrates that the gender distribution was relatively balanced, although there were more male participants than females in the German and Israeli focus groups. Figure 6 presents the age distribution of the participants in the three focus groups.

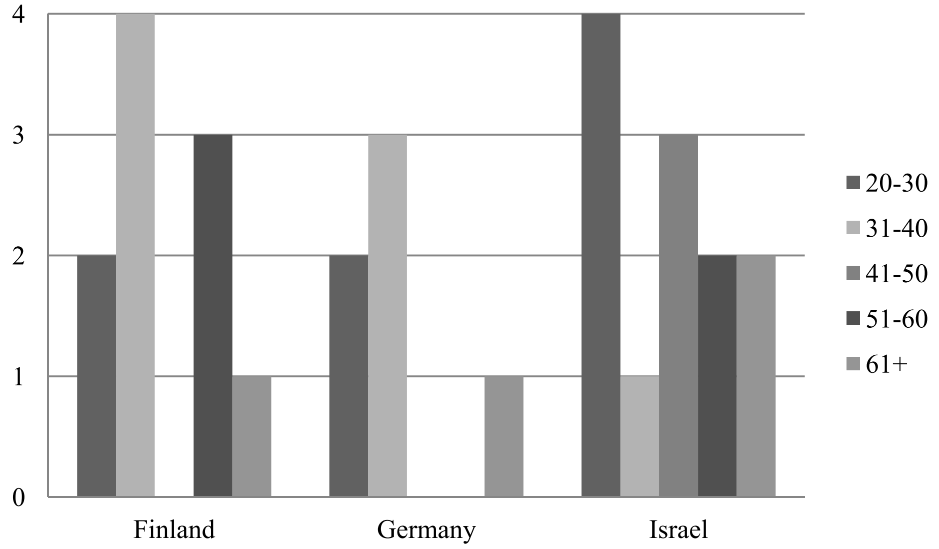

Figure 6 Age distribution of the focus group participants

Young adults and individuals over the age of 50 were rather well represented, while there were fewer participants who were aged between 41 and 50 years. The participants were from various backgrounds and none of them were experts or activists in the field of privacy. Therefore they represent the opinions of ordinary citizens rather than experts. The diversity and heterogeneity of the participants was a priority in the organisation of the focus groups. Firstly, the participants were of varied age, gender and education, although there was an overrepresentation of highly educated participants (Lobet-Maris et al., 2012, pp. 48–50). Secondly, the group was to consist of people from different backgrounds. A list of 18 affiliations was made to facilitate gathering a diverse focus group. The affiliations were the following:

1. Women’s association/group
2. Gay, lesbian and transsexual association/group
3. Unemployed people’s association/group
4. Family, parents association/group
5. Consumers’ association/group
6. Trade union association/group
7. Cultural association
8. Refugees’ association/group
9. Retired people’s association/group
10. Students’ association/group
11. Voluntary association, involved with the precarious people
12. Medical association
13. Secondary school teachers’ association
14. SMEs or enterprises’ association/group
15. Bar association
16. Officials’ / civil servants’ representatives or trade unions
17. Finance and Insurance sector associations
18. Members of parliamentary commission devoted to civil rights/privacy

(Lobet-Maris et al., 2012, pp. 77–78)

Of course it would be difficult to include participants from every category in each focus group. Nevertheless, no affiliations or age groups should dominate the focus groups, and both genders should have equal representation. As a result of the diversity of participants, the focus groups contain many different points of view, even though they cannot be said to represent the wider population in the sense of being a representative sample. For the purposes of this study, diverse points of view and the grounds given for them are more important than establishing typical opinions that could be linked to various background variables.

In the instructions for the focus groups, it was stated that the participants present their own opinions which are influenced by their personal background, but they do not represent a specific interest group as such. In addition, they were asked to speak about public concerns as citizens rather than telling personal anecdotes. The moderators, in turn, were asked not to introduce their own definition of privacy which would then direct the discussion. Instead, the aim was that the participants will approach privacy from their own perspectives to gain insight into their beliefs and understandings (Lobet-Maris et al., 2012, p. 78).

For the purposes of this thesis, the saturation of the images of the future is important. Saturation means that no important new points of view would be introduced by adding new participants. One central limitation of the thesis is that it is difficult to judge if saturation of points of view is reached. Ideally, additional workshops should be held where the participants' ideas would be tested and further probed and developed. This would make the results of the research more reliable and less prone to misinterpretation and random errors such as typing errors at the transcription stage. In addition, the validity of the central concepts used in the study could be corroborated. However, since the data will be analysed with qualitative methods which require extensive interpretation, a smaller number of participants is justifiable.

The focus group material will enable an analysis of how privacy is viewed and experienced by ordinary people in their lives. The analysis will then aim to go beyond the descriptive level, that is, beyond the self-understanding of the participants. The discussion in the focus groups is taken as a starting point from which to analyse the topic with the methodological and conceptual tools described in chapters 2 and 3.

The focus groups were analysed using thematic analysis with the aid of the Dedoose web application.[20] This means that the discussions are recontextualised into themes that are based on the hypotheses of the study and on the literature on privacy and images of the future (Ayress, 2008). The themes which were used were partly based on Bell and Mau's model of social change, partly on my own privacy dynamics model and partly on the literature on privacy (see Appendix 2: Themes Applied to the Empirical Material). Thematic analysis was used here as a strategy for data reduction with the aim of simplifying the data. The process can be described as analysis followed by synthesis. First important themes were collected from the focus group discussions and then these were reorganised into coherent clusters of participants whose images of the future were finally examined.

4.2 Potential Problems with the Focus Group Approach

There are two main challenges related to the focus group approach adopted here: the difficulty of the subject of privacy and the possible attitude-behaviour gap. Firstly, privacy is a difficult issue for non-experts to discuss in a focus group setting. Survey studies conducted in the United States have demonstrated that privacy is generally considered as important, but there have been concerns about systematic bias in the results due to two main reasons. First, those most concerned about privacy may not be willing to respond to surveys, which would underestimate the level of concern about privacy. Second, surveys that discuss only privacy may in fact influence people's views on privacy

[20] http://www.dedoose.com.

and cause them to form views that they did not hold before. Thus the results would overestimate the level of concern. In addition, in general questions about privacy it is not clear which context or aspect of privacy respondents are considering, thus raising questions about construct validity (Regan, 1995, pp. 49–51).

These concerns also apply to the focus group setting. The choice of participants is of course a central concern. In this case, the selection was meant to be widely representative but it was by necessity non-random. The narrow selection of participants cannot represent the larger population and any inferences beyond these individuals must be tentative. Of course, generalisability within qualitative research with a small number of participants is always problematic. The participants should thus not be taken to represent 'average' opinions within the population. Further studies would have to be made to study the generalisability of the results of this study.

An additional concern in focus groups is that the social environment of the focus group may cause an exaggeration of people's views and other social desirability effects. In other words, do participants claim to act or think in a certain way partly because of the social situation of the focus group? On the other hand, the focus group environment may encourage participants to speak about aspects which they would not mention if interviewed alone because topics may be raised by others and interaction and discussion is encouraged (Kitzinger, 1995, unpaginated). In my view, for the purpose of constructing ideal-typical images of the future, the positive aspects of focus groups outweigh the negative ones.

Moreover, it is difficult to know to what extent the participants are discussing the same issue when they refer to privacy. On the one hand, this ambiguity of the concept of privacy provides richness to the discussion, since every participant can introduce her own understanding of the concept. On the other hand, differences of opinion and misunderstandings may emerge simply because the participants are speaking about different things. The previous chapter discussed the multi-dimensional nature of privacy. Due to the complexity of the issue, the researcher should be aware of the context in which privacy is discussed in each case. The concrete example of the shopping centre scenario in the focus group questions (see Appendix 1: The Focus Group Questions) somewhat ameliorates this conceptual confusion, but at the same time it directs the participants' views to a certain aspect of privacy, namely its meaning in the commercial context as a kind of commodity.

A further problem with the focus group approach is that it cannot provide data on the actual behaviour of individuals. As Regan (1995, p. 58) notes, there are complex relationships between attitudes, cognitions and behaviours, particularly when discussing an abstract concept such as privacy. The focus group participants speak about how they *would* behave in certain situations and about their views on topics, but the focus group method cannot examine how people actually behave. Therefore, one should not make hasty conclusions about how people protect their privacy, for instance, based only on the discussions. As was already mentioned above, empirical research has shown that in privacy protection, individuals' attitudes and their actual behaviour differ markedly from each other (Acquisti, 2009). Of course, individuals' values are an important object of study even if they do not directly translate to behaviour. Considering the model of privacy dynamics presented above (p. 63), the focus group discussions present people's experiences, attitudes and internalised norms and provide hints about their privacy-related actions. They can also clarify what kinds of practices are perceived as violating privacy and in which contexts. More indirectly, the discussions may provide indications of social norms within norm circles, but these require interpretation and must be treated as tentative. Likewise the issue of legislation is not touched on extensively.

A final limitation concerns language. The Finnish focus group was analysed in the original language and sections were only translated for the final report. However, the German and Israeli focus groups were conducted in German and Hebrew, respectively, and English translations made by non-professional translators were analysed. Therefore the exact word choices of these focus group discussions must be treated with caution, and the focus should be more on broad themes than on specific vocabulary.

5 CONCEPTIONS OF PRIVACY: CENTRAL THEMES, THREATS AND SOLUTIONS

In this chapter, the focus group participants' conceptions of privacy and beliefs about privacy are analysed and the participants are clustered into four groups: privacy fundamentalists, privacy pragmatists, privacy individualists and privacy collectivists. First the process of analysis will be described, followed by a discussion of central themes and finally, the clusters of participants will be presented.

5.1 Process of Analysis

It was clear from the outset that there were many different perspectives expressed in the focus groups and there was no consensus on privacy and the futures of privacy. It was less clear how these differing perspectives could be analysed systematically. As I argued in my discussion of images of the future, an analysis of shared images of the future must begin with an analysis of the beliefs of individuals because then the connections between individuals' beliefs and their images of the future can be explored.[21] Shared images of the future are images shared by a group of individuals, a normative circle, though the circle can be widely dispersed globally and only communicate virtually.

The following method of analysing the focus groups was chosen. First, I analysed the views of each focus group participant separately and coded the material under themes based on three sources: Bell and Mau's model of social change, my own privacy dynamics model and the literature on privacy (Appendix 2: Themes Applied to the Empirical Material). Then, I looked for themes where opinions differed in a distinguishable way. Finally, I sought commonalities between the individuals in order to cluster the participants into four groups in a qualitative and subjective manner. The aim was that there would be less variance in perspectives within groups than between groups. The clustering process is described in more detail in section 5.3.

In this chapter, I will present the themes and the clusters. There are five central themes where opinions differed and which are theoretically relevant for this research. First, what is the conception of privacy and of the functions of privacy? Second, what are seen as threats or drivers of change? Third, which actors are seen as responsible for

[21] An alternative approach would be to examine conceptions of privacy and images of the future as discourses separated from individuals. In the approach I have taken, the individual is an important point of reference because individuals′ beliefs are linked to their images of the future.

protecting privacy? Fourth, what kinds of solutions are presented? Finally, are individuals seen to have control over sharing personal information or is control an illusion?

In the next chapter, the images of the future of the four clusters of participants will be explored, building on the focus group discussions but combining the views of participants into ideal-typical composites. Furthermore, the relations between the conceptions of privacy and the images of the future will be analysed. In a sense, then, this chapter deals with the parts of individuals' subjective models of privacy dynamics and the next section will discuss these subjective models as a whole and the related images of the future.

5.2 Central Themes

5.2.1 Conception of Privacy and the Functions of Privacy

The first dimension where different opinions were raised is the overall conception of privacy and the connected question of the functions of privacy. Many different individual conceptions of privacy were presented, many of which corresponded with theories of privacy, which suggests that privacy theories grasp at least some aspects of the subjective experience of privacy. Privacy was considered from both normative and descriptive points of view. Most participants in all three focus groups agreed that privacy is important, although considering Regan's critical comments about survey responses this could also be caused by situational factors. According to Regan (1995, pp. 49–50), discussing any issue separated from other issues tends to lead to it being given high importance.

Views on the importance of privacy ranged from those regarding privacy as an eternally important value to those that viewed privacy in more pragmatic terms. A German focus group participant (female, 31–40 years) stated that privacy will be "eternally an important value", while a Finnish participant (female, 51–60 years) held that privacy is "important but not grave [extremely important and serious]".

Most participants discussed privacy in relation to both information and spatial access, suggesting that both aspects are important. Perceptions of the scope of privacy also varied. Some participants defined privacy very widely: all information that they wish to keep private should remain private. A Finnish participant argued that it should be possible to keep private all such information that does not harm others or does not pose a threat to their security (male, 21–30 years). Similarly, a German participant stated: "I protect everything. Strangers must not know anything about me" (male, 61+ years). An Israeli participant also expressed a similar view, asserting that everything that he wishes to remain private should be private (male, 21–30 years). One participant argued that her information must be protected because it is generally used for the benefit of others rather than her own benefit (female, 31–40 years, Finland). From this perspective, the general principle is that most information about an individual is nobody else's business. This is similar to John Stuart Mill's conception of autonomy where an actor's self-regarding actions are nobody else's business (Räikkä, 2007, p. 44).

Spatially, the home was commonly seen as a private area. Some participants seemed to advocate a rather strict private/public divide, arguing that everything they do in public places is public. One German participant (male, 31–40 years) stated that "information that I published is irretrievably public" and "as soon as I am leaving home I am in public space where everybody can see what I am doing". These are in effect corresponding statements indicating a strict divide between private and public, the first one referring to information and the second one to space. The same participant held that the core of privacy is control over access:

> *Privacy is reachability. To me it is a simple formula: everybody can know everything about me as long as he cannot call and disturb me. I don't mind as long as I have the control over who approaches me when because they have only the data that I have given to them. Privacy is to me a controllable good – I control who approaches me when. This is my definition of privacy! I decide when I am a private person and when I am a public person.*

The primary concern, then, is with access because control over information is seen as unproblematic. There is marked contrast to the "protecting everything" approach. This participant also viewed privacy protection as protection of mental integrity and likened it to the protection of physical integrity. From this perspective, intrusions into one's home or one's personal space are practices that violate privacy. Practices related to information are not seen as equally intrusive. Another participant also emphasised similar aspects, arguing for example that collecting data about shopping in a shopping centre is not a violation of privacy because he is in any case similar to all the other shoppers (male, 31–40 years, Finland). This theme can be linked to the question of control, discussed below. Perhaps if a person feels that she has control over her information, practices related to information are not seen as a problem, whereas if control is seen as illusory, informational practices are much more threatening because our information may be spread without our knowledge and control.

Privacy was, then, commonly linked to the home. Other characterisations were privacy as a "retreat area" (three participants in the German focus group) or as a "nest" (male, 51–60 years, Finland). Warren and Brandeis expressed this notion in the 1890s. According to their classic article, the "intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world" (1890, p.

196). Stanley Benn expresses a similar view and links it to identity: “We need a sanctuary or retreat, in which we can drop the mask, desist for a while from projecting on the world the image we want to be accepted as ourselves, an image that may reflect the values of our peers rather than the realities of our natures” (1971/1984, p. 241).

On the one hand, privacy as a retreat is negative: there should be a space where the individual is let alone, as two participants argued (male, 31–40 years, Germany; male, 51–60 years, Finland). In this retreat area, the individual can be who they are without being “confronted with external expectations” (male, 31–40 years, Germany). This is essentially the same conception as the classic definition of privacy as “the right to be let alone”, which Warren and Brandeis quoted in their influential article (Warren & Brandeis, 1890). This theoretical tradition has continued since then in the limited access or restricted access theories. The freedom from “external expectations” is very similar to Schoeman’s notion of freedom from overbearing social scrutiny and regulation. In this conception, the real self behind social roles needs a space, the private world, to be what it is and to have dignity (Schoeman, 1992, p. 133). One participant spoke explicitly about identity management: “I have a social image, the way society sees me, and there is my inner self. Anything I don’t want to include as part of my social image is private” (male, 21–30 years, Israel). In this sense, privacy is seen as crucial for identity but essentially as seclusion and separation from society.

On the other hand, some participants also saw the positive side of this retreat: the increased possibilities of freedom and autonomy. For example, a German participant stated: “in the job I have to conform to regulations, *at home I can do what I want*” (male, 61–70 years). Another German participant argued that privacy is “a retreat area and the collection of personal features and attributes that *gives me the opportunity to act freely*” (male, 31–40 years). A third participant in the German group held that privacy gives him “the space to behave in a room without existing guidelines” (male, 21–30 years). One crucial function of privacy that was identified is to maintain autonomy and liberty. This is in accordance with my own conception of privacy as maintaining boundaries between normative circles in order to protect social freedom and autonomy. As Schoeman (1992, p. 156) argues, privacy is often privacy *for* something in addition to privacy *from* someone.

Many privacy theorists see the protection of intimacy and intimate relationships as the function of privacy. Privacy does not only enable freedom to act autonomously but freedom to act together with others and to form and maintain relationships. Some participants emphasised the connection of privacy and intimate relationships such as those with one’s partner or with one’s friends. In general, issues related to family were seen as private issues. One participant in the Finnish focus group (male, 21–30 years) raised the importance of being able to control which information you share with which person. According to him, the meaning of sharing is lost if everything is already public. In addition, sharing with close friends should be spontaneous and not in exchange for something else. This conception is close to the privacy theories of Fried and Rachels which emphasise differential sharing to enable maintaining different kinds of relationships (Fried, 1968/1984; Rachels, 1975/1984).

Trust was also a common theme in the focus group discussions. Privacy has a complicated relationship to trust, and this was apparent in the focus groups as well. Solove notes as a disadvantage of privacy that privacy makes establishing trust more difficult (Solove, 2008, p. 81). On the other hand, Charles Fried argues that privacy is a necessary context for love, friendship and trust (1968/1984, p. 206). It can be argued that privacy is a precondition for trust, since privacy makes it possible in theory to betray trust. If there were no privacy and all thoughts and actions were public, there would be no need to trust one another and betraying someone's trust would be impossible even in theory. As Fried argues, "[t]here can be no trust where there is no possibility of error" (1968/1984, p. 212). Two participants in the Finnish focus group emphasised that sharing information requires trust, that is, trust is needed in exercising control over information (male, 51–60 years; female, 31–40 years). According to one participant, if this trust were betrayed, it would lead to an experience of loss of control (male, 31–40 years, Finland). Two participants, in turn, argued that meaningful sharing with others builds trust in interaction (male, 21–30 years, Finland; female, 21–30 years, Germany). Sharing, then, both requires trust and builds trust. Privacy as control over sharing is seen as a necessary context for building this trust through voluntary sharing.

Personal relationships are clearly important for sharing information. Reciprocity in these relationships was seen as important. For example, one participant argued that there was a personal relationship with shop owners and there was a reciprocal relationship where both knew each other (male, 61+ years, Germany). A Finnish participant, in turn, mentioned that the owner of a shopping centre which collects customer information would probably not want to be followed in his daily activities (male, 21–30 years). Several participants stated that they do not want to give their information to strangers or anonymous contact points such as shopping centres and institutions. This could be called particularised trust, as opposed to generalised trust. Particularised trust refers to trusting those with whom one is interacting. At the extreme end, one participant stated that he trusts no one and he is "fanatical" about keeping intimate information to himself (male, 51–60 years, Israel). This is similar to James Rachels's notion that there must be a particular relationship for information about oneself to be someone else's business (1975/1984, p. 297).

Generalised trust, in contrast, refers to trust in institutions and in fellow people in general. One participant noted that we have in effect expanded our trust to credit card companies and Facebook, for example (male, 21–30 years, Israel). It is, of course, a separate question how consciously this expansion of trust has happened. Concerning organisations, one participant stated that she trusts government much more than business, while another participant expressed more trust towards companies than government (female, 21–30 years, Germany; male, 31–40 years, Finland). Interestingly, both cited similar reasons: clear regulations and good practices. With the government, practices are perhaps more transparent, but on the business side there is another incentive to protect privacy: if a firm engages in violating practices and is caught, it may lead to loss of business and eventually bankruptcy.

While personal relationships were emphasised, the possibility of anonymity was also seen as positive by several participants. In an interesting variation on the theme of trust, one participant argued that information should really be protected from those that one knows, because to strangers one is in effect anonymous (female, 31–40 years, Finland). Another participant made a similar point, telling a story about a school headmaster who had to ride his bicycle to another town to avoid being seen in a shop selling alcohol (male, 31–40 years, Finland). According to this perspective, sharing of information is not a problem when there is no personal relationship and no context for the information, a kind of mirror image of James Rachels's argument. This is because a person's sensitive information only has meaning for those close to her, which in turn comes close to Jeffrey Reiman's argument about the context of caring which is more important than information as such (1976/1984, p. 305). Information then only needs to be kept private from those people, not from everybody. It must be stated, however, that this requires an environment where anonymity is possible. Perhaps it could be argued that these contrasting views on intimacy reflect an underlying consensus that intimacy is the context in which private information is meaningful. In the former approach, privacy is linked to more or less all personal information, while in the second approach the context of intimacy is required for information to be private.

The focus on intimate and personal relationships arguably emphasises the seclusion aspect of privacy, with the difference that intimate friends or partners are secluded from society rather than the individual. There were also some comments about the wider social importance of privacy. One participant (male, 31–40 years, Germany) argued that privacy is a cultural value that is connected to the Enlightenment and a political value as "part of the protection of citizens which is one of the main tasks of society and the state". Furthermore, this is seen as important for maintaining democracy. The same participant also argued that social control and exclusion mechanisms can only work if organisations can access our private information freely and therefore privacy must be protected in order to prevent social exclusion. An Israeli participant (female, 21–30 years) made a similar argument, stating that privacy protects from inequality. Without privacy, everybody would have a different "colour" and could be treated differently. She adds that privacy must be uniform: "everybody must be exposed or concealed in the same amount". Another participant argued that privacy protects against discrimination (female, 31–40 years, Germany). Participants in the Finnish focus group were also concerned about equality and the protection of those who are less able to protect themselves, such as young people and disadvantaged people.

These arguments link with all three of Priscilla Regan's aspects of the social value of privacy: privacy as a common, public and collective value (see p. 46). Firstly, viewing privacy as a cultural value implies that it is shared among most people and thus it is a common value. Secondly, privacy as a public value enables citizens to come together as equals to form the 'public', because people's private differences are not in everyone's knowledge and thus cannot be exploited. Finally, the reference to equality suggests privacy as a collective value. The difference is that in the normative argument that was presented everybody *ought to* be exposed in the same amount, while Regan in effect argues that everybody *is* exposed in the same amount, because in reality privacy is a collective good.

There was also disagreement on the topic whether privacy is a commodity that can be traded in exchange for goods. According to Nissenbaum, Julie Cohen has expressed concern about the trend of framing privacy increasingly as a marketable commodity which ignores its crucial function in promoting moral autonomy (Nissenbaum, 2010, p. 76). Many participants strongly expressed that privacy is not a commodity and that their information is not for sale, while others were more pragmatic and stated that information can be and is exchanged for benefits such as more efficient services and targeted marketing. In general, those who argued that privacy is not a commodity seemed to be concerned about their information as something valuable, whereas more pragmatic participants questioned the value of their personal information. This suggests that those most concerned about privacy view privacy as priceless, that is, not to be sold at any price.

The issue of conceptions and functions of privacy is thus rather complex and no two participants' opinions are identical. However, I would argue that the following four broad groups of privacy conceptions could be identified:

1. Privacy is the right to be let alone and control over personal information. Informational privacy has a wide scope. Privacy has functions primarily for individual identity and for maintaining intimate relationships.
2. Privacy is a shared value which is important but not extremely serious. It is difficult to articulate why privacy is important.
3. Privacy is different things for different people. It can be controlled, negotiated and traded with.
4. Privacy is control over information and access, but it is also an important value connected to autonomy and the maintenance of democracy. It is a shared, public and collective value.

5.2.2 Threats to Privacy

Privacy threats were discussed on a general level as well as examining threats to the personal privacy of individuals. Alternatively privacy threats may be called drivers of change if one wishes to use a more neutral term. Many participants cited lack of information and awareness about risks as a central threat to privacy. One participant argued that we have a false sense of security when we are at the computer and we are in fact exposed (male, 31–40 years, Israel). It was also noted that we do not care about privacy violations because they are in the small print of contracts and thus invisible to most people (female, 31–40 years, Israel). Lack of knowledge is related to uncertainty: we do not know how data collected today may be used in the future (male, 21–30 years, Germany).

A complementary perspective to lack of knowledge is the lack of transparency from companies and institutions. This is similar to the lack of knowledge argument, but here the responsibility is on the organisations rather than the individuals whose privacy is at stake. From this perspective, it is the organisations' responsibility to provide necessary information for individuals to make informed decisions relating to their privacy such as what to share on a social networking site. Several participants stated that they want more transparency from organisations handling personal information.

New technologies were seen by some participants as a driving force but overall they did not feature very prominently in the discussions. One participant noted that new technologies enable spreading our information without our knowledge, and another noted that there may be ethical issues when technologies start affecting the human brain and affecting our autonomous decisions (male, 51–60 years, Finland; male, 61+ years, Israel).

However, many participants were aware that technology is progressing rapidly. The notion of legislation lagging behind technological development was expressed in all three focus groups. The view was expressed that in the market, needs of producers and consumers meet each other through technological developments and more efficient services, and legislation is likely to be two or three parliamentary terms behind real developments in privacy (male, 31–40 years, Finland). Another participant noted that legislators cannot avoid dealing with privacy policies even though they will lag behind technological developments (male, 31–40 years, Germany). In addition, one participant stated that since the government currently lags generations behind the development, it is difficult to say whose responsibility privacy is (male, 21–30 years, Israel).

Participants also noted that current laws have loopholes and deficiencies. One Finnish participant (female, 31–40 years) was concerned about exceptions in data protection laws, while another participant stated that the internet is a vast grey area when it comes to law (male, 21–30 years, Israel). An Israeli participant noted that there are open spaces and room for interpretation in laws, which creates problems (male, 51–60 years).

In terms of actors threatening privacy, participants mentioned traditional security threats such as criminals and hackers. Large corporations which aggregate and sell personal information were also mentioned (female, 31–40 years, Finland). One participant stated that there are potentially many actors threatening privacy depending on the situation: the state, an employer, someone ridiculing one online or simply some unknown person (male, 21–30 years, Finland). The final comment, threats from unknown others, is important because it relates to a contemporary argument about privacy. According to Mika Mannermaa, surveillance is no longer done by any Big Brother alone but by a diffuse ‘some brother’: public actors, companies and private citizens. This surveillance can be either benign or threatening (Mannermaa, 2008, p. 35). The key difference is that we no longer know who exactly the threat is. Surveillance is done by many actors with various interests. The democratisation of access to databases has been an important part of this development (Nissenbaum, 2010, pp. 38–40). In addition, one participant stated that institutions out of reach of the individual are a threat, implying that impersonal relations with companies and public actors create privacy risks (male, 31–40 years, Germany).

On the topic of interests, the threats that were identified were quite traditional: the commercial interests of companies and the security interests of states. However, some participants saw no reason to be afraid of business and saw little commercial value in their information. From this perspective, the government and other public actors can be more threatening because they have access to many kinds of information about individuals.

Another kind of danger to privacy was seen in norm change. According to this perspective, privacy becomes less valued as new generations share more openly. The implication is that these young generations are not aware of the dangers. In fact, one Israeli participant claimed that the open communication of young people is against human nature (male, 61+ years). This point of view suggests that hedonism and loss of morality among young people are threats to privacy.

Concerning perceived threats to privacy, the participants can be divided into four broad groups:

1. There are many threats to privacy, such as companies with commercial interests, governments and other individuals.
2. Traditional threats such as criminals.
3. New technologies challenge privacy. Government is a more serious threat than business.
4. Lack of awareness, knowledge and transparency are the main threats.

5.2.3 Individual or Collective Protection of Privacy

The third crucial difference between focus group participants was concerning responsibility for protecting privacy. Concerning this issue, participants could be divided into two groups: those who argued that individuals should primarily protect their own privacy and those favouring collective solutions such as legislation. In the discussions, these alternatives were not mutually exclusive. Most participants saw some role for both individual and collective privacy protection but there were nevertheless clear statements in favour of either one approach or the other. For the sake of creating ideal-typical images of the future, it is useful to treat the two as alternatives emphases. Another way of expressing this question is whether individuals and the state are seen as active or passive in protecting privacy.

The role of the state in protecting privacy was emphasised by several participants in both the German and Israeli focus groups but the theme was somewhat missing from the Finnish discussion, except for one statement that the law in Finland currently protects privacy rather well. The likely explanation for this is that the voluntary sub-questions about whether privacy is a psychological or political issue and whether privacy protection is primarily individual or collective were not asked in the Finnish focus group due to time constraints. Additionally, in the Finnish focus group, the participants were asked whether they felt *their* privacy was in danger rather than privacy as such. This inevitably framed the discussion in more individualist terms. These facts raise some questions regarding the comparability of the different focus group sessions. On the other hand, Finnish participants could have raised viewpoints emphasising collective protection of privacy even in this case if they felt strongly about the issue. Moreover, none of the participants are categorised into clusters on the basis of this variable alone.

It could be simply coincidental that the theme was not explicitly discussed in Finland, and it is even possible that the role of the state is obvious for Finns and therefore they did not feel the need to discuss it. However, for my purposes, the focus group discussions will be treated as a whole and the reasons for cultural differences will not be examined. With relation to the state's role it was emphasised that the government should offer information and to offer regulations against institutions and organisations to protect personal data (female, 31–40 years, Germany; female, 21–30 years, Germany). One participant stated that the government should regulate people's measure of exposure in a similar way than the quality of food and medicine are measured (male, 61+ years, Israel). The state is thus seen by some participants as a protector of privacy and of the autonomy of individuals. At the same time, the limits to government power were emphasised: the government should not "act paternalistically" and it should not limit individuals in handling their personal data (female, 31–40 years, Germany; male, 31–40 years, Germany). Participants tended to speak of 'the government' in a rather undifferentiated way. This category can be seen to cover all public actors such as public officials and data protection authorities in addition to the government as such.

Those emphasising the role of the individual argued that personal responsibility should be promoted and that people should be as free as possible within a minimum framework that protects people from themselves (female, 31–40 years, Israel; male, 21–30 years, Germany). According to one participant, some regulation is needed but “basically, it is a personal matter and everyone must do whatever one can” (male, 51–60 years, Israel). One participant likened privacy to property and argued in the following way: “I think it’s a combination**.** I am responsible to do anything in my power to protect my privacy, like I do with my personal property, but once it is compromised, it’s the state’s responsibility to deal with those who did it, just like it has to do when my car is stolen, for example” (male, 21–30, Israel). In addition, one participant mentioned the voluntary sector as a potential provider of education to teenagers (female, 31–40 years, Israel). It is important to remember that there are limits to how much individuals can protect their privacy with their own actions. Individuals always act within a certain social setting with certain societal power relations. In de Jouvenel’s terminology, many futures which are dominating for individuals can be masterable collectively.

While many participants emphasised a balance between individual and collective protection of privacy, participants can nevertheless be roughly divided into two groups on this issue:

1. Individuals are mainly responsible for protecting their own privacy.
2. Individual protection is insufficient and there should be a regulatory framework for privacy protection.

5.2.4 Solutions to Privacy Threats

Solutions to privacy threats can be categorised based on whether individual or collective protection of privacy was emphasised. Solutions are of course also linked to whether privacy is viewed as threatened and how the threats are seen to emerge. Some solutions can be called individual coping strategies for managing a situation where privacy is at risk. For example, two Finnish participants stated that they had used means such as deleting their name from their postal box, having no address in the telephone directory and placing marketing bans. The term coping strategy is used because individuals have to change their ordinary ways of behaving because of privacy threats. By using such strategies, particular privacy threats may be averted but the systematic practices that violate privacy remain unaffected. One participant stated that if she felt that Facebook was threatening privacy, she could delete her account (female, 21–30 years, Finland). Of course, one person deleting her Facebook account has no effect on systematic threats to privacy but if many consumers decided to abandon such services, there could be an effect. Other participants emphasised common sense and personal responsibility. There can be seen as attitudinal coping strategies of individuals. Many participants also saw professional confidentiality and the requirement of consent in European legislation as efficient privacy protection mechanisms.

Of course, consent is effective only if there is enough information. Since lack of knowledge and awareness was seen as a central problem, it follows that raising awareness is presented by many participants as a solution. The implication is that by gaining information, individuals can behave more responsibly regarding their own privacy. The responsibility then is on individuals, but also on public actors to provide education and information and on companies to increase transparency about practices. Two Finnish participants agreed that continuously discussing privacy and maintaining its salience as an issue helps to protect privacy (male, 21–30 years; male, 51–60 years).

Some participants offered obscurity and lack of interest as a mechanism that protects privacy. This is similar to Gavison's argument that privacy is largely protected because there is no interest in violating it (1980/1984, p. 379). In the focus groups, there were in fact two distinct arguments concerning protection by obscurity: a qualitative and quantitative one. The qualitative argument states that individuals are safe in public places and their information is safe because they are similar to others and therefore uninteresting. Three participants made the argument that the privacy of ordinary people, as opposed to celebrities, is not under threat because there is no interest in them (female, 31–40 years, Finland; female, 51–60 years, Finland; female, 31–40 years, Germany). The quantitative argument was provided by one German participant and it states that companies are interested in aggregated datasets about large numbers of individuals, and due to the amount of data, traceability of individuals is unlikely (male, 31–40 years).

As far as interests are concerned, the arguments may hold, but technologically, protection by obscurity can be seen as endangered. Nissenbaum (2010, p. 37) is sceptical about the possibilities of privacy by obscurity, claiming that it is no longer possible due to the massive and deep databases that have been developed. Certainly computer processing power and search algorithms are constantly progressing, and therefore what seems to be an enormous amount of data today may be easily processable in the future. However, it could be argued that in practice many people still feel relatively anonymous within the city. This urban anonymity was seen as positive by three participants (male, 31–40 years, Germany; male, 21–30 years, Finland; male, 61+ years, Finland). It could be argued that at the moment forced loss of anonymity only concerns certain kinds of information such as shopping. Of course the question remains what the possibilities for anonymity and obscurity are in the future.

All of the solutions mentioned above are more or less solutions either enacted by or aiming at individuals. In contrast, some participants explicitly stated that it is important to have legislation and a regulatory framework for privacy protection. For instance, one German participant stated that "privacy is and must be legally protected" because it protects individual self-determination (female, 21–30 years). Two participants emphasised the right to drop out or the right not to give information (male, 21–30 years, Israel; male, 21–30 years, Israel). However, the obvious question about such a right is whether a person could 'drop out' from the school system, for instance, and where the individual would drop if they opted out of systems crucial for public administration. In addition, several participants emphasised that there must be consequences if the law is broken.

Only one participant offered corporate self-regulation as a solution, stating that companies which violate privacy quickly lose their customers (male, 31–40 years, Finland).

Summing up the solutions to privacy threats, four broad groups could be identified:

1. Personal coping strategies, common sense and personal responsibility
2. Raising awareness through education, information and discussion
3. Anonymity, obscurity and lack of interest in ordinary people
4. Privacy legislation: a broad regulatory framework.

5.2.5 Control over Privacy: Reality or Illusion

In the chapter on theories of privacy, it was mentioned that one of the most influential definitions of privacy is privacy as an individual's control over her personal information (Westin, 1967, p. 7). Variations of this theory view privacy as control over intimate information and control over access to oneself (Fried, 1968/1984; Rachels, 1975/1984). The control theory of privacy has since been viewed as overly subjective and limited, and Nissenbaum's contextual integrity theory, for instance, views control as merely one possible information transmission principle. However, in all three focus group discussions, control was one of the most often mentioned general themes. This is unsurprising, because the issue of control directly relates to the experiences and actions of ordinary citizens unlike data protection legislation, for instance.

Many aspects of control were explored in the discussions. On the issue of control, participants can be divided into two groups: those who believe that individuals can exercise control over information or access and those who believe that control is an illusion. Participants within the first group believe that they can generally decide what data they are sharing and see no issue with control. The second group saw control as more problematic: it is wishful thinking or illusory. One Israeli participant even proclaimed that her assumption is that everything about her is already known and she has no control over it (female, 41–50 years). A few participants were less clear about the issue of control. They either did not mention it or mentioned it in a normative sense, that we *should* have control. No participant explicitly stated that control is not important in their view.

The experience of control or lack of control is crucial because it is an indicator of whether privacy harms are experienced. If an individual feels she has enough control over her privacy, privacy is overall a much less problematic issue than if loss of control is experienced. Privacy can be seen as important even if we can control it, but it is not seen as an issue in the same sense than if control cannot be exercised.

Another issue is that it is not always easy to distinguish between the *experience* of control and *actual* control. Crucially, participants who questioned the possibility of control questioned actual control, not the experience of being in control. One Israeli participant, for instance, stated that we are only seemingly in control, referring in particular to the fact that Facebook can alter its privacy policy at any time and most people will not abandon the service in this case (female, 31–40 years). The illusion of control and false security relate to the lack of knowledge that was mentioned above as a central threat to privacy. Control arguably also has two aspects: control over initial sharing and control once information has been shared to a limited group. Certain participants were sceptical about having control once information is shared while others considered that there is no control to begin with. One participant referred to the notion of controlling information after it has been shared with somebody as "wishful thinking" (female, 31–40 years, Finland). Control is thus a complex issue involving degrees and kinds of control rather than simply having or lacking control.

However, these complicating factors were not considered in the clustering of participants because it would have led to very small clusters. The final dimension for comparing participants, then, is whether individual control over privacy is seen as real or illusory.

5.3 Combining the Dimensions: Clusters of Participants

The opinions of focus group participants differed regarding various theoretically relevant dimensions of privacy. However, I would also argue that the various dimensions tended to vary together so that a particular conception of privacy is united with a particular view of threats and solutions, for example. Moreover, they tended to coincide with particular beliefs about the future, as will be argued in the next section. Divided along these dimensions, four clusters of participants were identified within the focus groups. Two initial remarks need to be made about the composition of the clusters. Firstly, all clusters except for one include participants from all countries and all clusters included both female and male participants. Cultural and gender differences thus do not seem to play a significant role regarding these dimensions among this set of participants. Secondly, the cluster of those most concerned with privacy is significantly larger than the others, which corroborates the hypothesis that participants are likely to be concerned with privacy, possibly more so than the overall population.

The clustering of participants was based on the thematic analysis of the material and on the five dimensions of privacy conceptions that were discussed in the previous sections. However, since the empirical material consisted of loosely structured focus group discussions, much interpretation and subjective judgment had to be used for composing the clusters. The clusters were formed using a combination of previous knowledge based on the literature, the empirical material and subjective judgment. In the beginning there were certain hypotheses about types of privacy conceptions and the systematic study of the empirical material refined and altered these hypotheses.

The process began with identifying participants that clearly differed from each other and placing these participants in different clusters. Then participants that were somehow similar to these initial 'cluster centres' were placed into the clusters. Not all participants expressed views on all dimensions of privacy conception. In addition, as with all qualitative material, there were some contradictory views and difficult cases. Nevertheless, I attempted to make the clusters as coherent as possible using the information that was available. In general, participants expressed one or more views that placed them in one of the clusters. The hypothetical 'cluster centres' or typical views also shifted somewhat as more participants were included in the clusters. I would argue that ultimately a relatively coherent clustering emerged from the material, but this clustering could of course be refined or questioned using additional empirical material. Table 4 below presents the clusters with the related variables.

Table 4 Clusters of participants

Cluster	***Conception of privacy***	***Threats***	***Responsibility***	***Solutions***	***Control***
1 ***(n = 12)***	Right to be let alone and wide control over personal information. Functional for protecting the individual and maintaining intimate relationships	Many threats: companies, governments, individuals.	Individual	Personal coping strategies, personal responsibility. Anonymity. Raising awareness.	Illusory
2 ***(n = 5)***	Privacy is an important value but not extremely serious. It is difficult to articulate why privacy is important.	Traditional threats such as criminals.	Both	Common sense, traditional mechanisms.	Real
3 ***(n = 4)***	Different things for different people. Privacy can be controlled, negotiated and traded with Functional for protecting the intimate sphere	New technologies. Government is a more serious threat than business.	Individual	Common sense, personal responsibility. Obscurity.	Real
4 ***(n = 7)***	Control over information and access but also a shared, public and collective value. Functional for maintaining autonomy and democracy.	Lack of awareness, knowledge and transparency are the main threats. Companies, governments.	Collective	Broad regulatory framework. Raising awareness.	Real

The Harris-Westin surveys on privacy segmented the public into three groups: privacy fundamentalists, privacy pragmatists and privacy unconcerned (Westin, 2003, p.

445). Following this terminology, I will call the first cluster *privacy fundamentalists*.[22] Clusters two and three are quite similar. The main difference between them is that participants in cluster two tended to strike a balance between an emphasis on individual and collective protection of privacy, while participants in the third cluster tended to be more individualistic. Thus cluster two will be called *privacy pragmatists* and cluster three will be called *privacy individualists*. The fourth cluster is called *privacy collectivists*. There were no participants in the focus groups that could be called privacy unconcerned. This is expected, since those unconcerned with privacy are unlikely to attend a focus group on the topic.

[22] However, the privacy fundamentalists here differ from Westin's usage of the term. For Westin, privacy fundamentalists support legal and regulatory privacy protection, while here the term is used to refer to participants who showed a deep concern for privacy but less focus on legal regulation.

6 IMAGES OF THE FUTURE OF PRIVACY

The previous chapter focused on subjective views that individuals have about privacy and changes in privacy: their beliefs about the past, beliefs about the present and beliefs about cause and effect. This chapter aims at connecting these beliefs with the participants' views on the future. Both the beliefs and the images of the future are discussed in terms of the clusters that were identified in the previous chapter. In the following, the process of analysis will first be briefly described, then the images of the future are presented and analysed via causal layered analysis. A general discussion of the images of the future and of their implications will conclude the chapter.

6.1 Process of Analysis: Causal Layered Analysis and the Privacy Dynamics Model

Causal layered analysis enables a systematic discussion of the assumptions behind the future-related beliefs of individuals. In causal layered analysis, the studied images of the future are divided into four layers: litany, system/social causes, discourse/worldview and myth/metaphor. The litany level is the surface-level understanding which takes an issue as given and does not examine its connections with other issues. An example of a litany understanding of privacy is that privacy is already lost because the state and large companies know everything about citizens. The system level explores the social, technological, economic and other causes related to the phenomenon. Systemic connections are examined but the larger paradigm is not questioned. For instance, privacy may be diminished because there is a growing network of surveillance cameras, which in turn reflects the growing power of the state and security companies in monitoring citizens. On the worldview level, the deeper ideologies and actor-invariant processes are examined. For example, surveillance cameras can be seen as a form of protection against terrorism and other risks. The final myth level includes the shared stories and metaphors to which individuals are deeply committed. These stories are not necessarily easily expressed in language but they are nevertheless crucial for the formation of cultural identity and for organising the anticipation of futures. Myths are the stories which give meaning to disconnected events and structure them into a larger whole. The layers should not be simply analysed separately, but movement back and forth between the layers is crucial in CLA (Inayatullah, 2004a, pp. 11–15; Patomäki, 2006, p. 8; Schwartz, 1996, pp. 39–43).

The layers of causal layered analysis are illustrated in Figure 7.

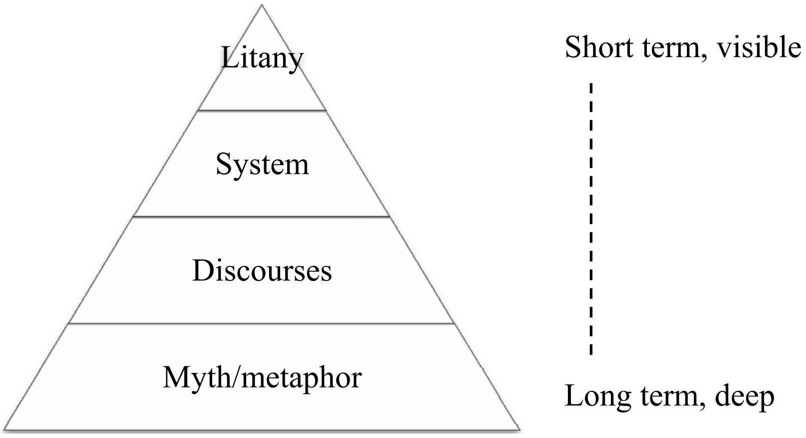

Figure 7 The causal layered analysis pyramid (Inayatullah, 2004c)

The figure is shaped as a pyramid to suggest that the bottom layers are more comprehensive and actors are less conscious of them. Therefore, changing them requires more time. As I argued in section 2.3, causal layered analysis is used here as a tool for analysing subjective perceptions. From this perspective, it is compatible with a critical realist theoretical framework. In this study, the CLA layers are used to analyse the focus group participants' images of the future and to examine how they are influenced by their beliefs about the past, the present and about causes and effects.

The challenge for this study is that the focus group material is collected primarily for analysis with methods other than CLA. According to Inayatullah (2004a, p. 6), the CLA process "must be communicative: the categories need to be derived through doing in interaction with the real world of others – how they see, think, and create the future". Ideally, CLA should thus be used in a context where the researcher can ask further questions and explore the different layers of the participants' understanding. In this study, this dialogue will need to be imagined. However, the focus group material may be a rich source of qualitative data even though it is not collected specifically for a causal layered analysis. In addition, while CLA in general promotes learning among the participants, the approach here is more traditionally scientific. The aim is to understand presently held beliefs about privacy rather than explicitly trying to improve them.

Of course the real determinants of one's image of the future are very complex, consisting of aspects adopted from one's social environment, one's personal attitudes regarding various issues and so forth (Rubin & Linturi, 2001). In addition, an individual can have many images of the future which may be contradictory and in conflict with each other (Rubin, 2013, p. S40). In this study, I have tried to simplify matters for analytical purposes by creating ideal-typical composites of the views of participants with similar views on privacy. Therefore these images are not promoted by any individual in exactly the way they are presented here and their features may be somewhat exaggerated. The intention is to present each image of the future as an ideal type of a particular perspective on privacy in the future.

In the following, each participant cluster's conceptions are first summarised in a table which is followed the narrative of the image of the future and then by another table summarising the causal layered analysis of the ideal-typical image of the future. The narrative of each image of the future is collected from the participants of a particular cluster with only small alterations to produce a coherent text. Because most of the narrative text is from participants, exact references to participants are omitted. The causal layered analysis which follows the narrative includes a great deal of interpretation, with references to literature and to participants' views where appropriate. Certainly other conclusions with regard to myths, for example, could also be drawn from the same material.

The privacy dynamics model, presented above (p. 62), is used as a frame of reference in the analysis. The participants' views relate to the model in two distinct ways. Firstly, they represent individual experiences and internalised norms which are part of the model. Secondly, I will argue that each participant cluster presents a subjective version of the entire model. That is, they have subjective views on the key actors, interests and privacy norms, for instance. These views fit into the system layer of causal layered analysis. However, these 'subjective models' are discussed on a fairly general level because on the whole, participants did not discuss them extensively. In addition, some clusters presented clearer views on systemic aspects than others.

As a final remark before proceeding to the images of the future, it is important to be precise about what is studied in the images. In the section on privacy dynamics, it was argued that the objective circumstances and possibilities for having privacy are more important from the social perspective than the exact ways in which individuals choose to exercise their privacy. The future of privacy is viewed as the future of a social institution with a changing surface level but a relatively stable underlying form. Changes in privacy are viewed from this perspective as changes in norms, legislation or societal practices.

Therefore, the images of the future are *subjective perceptions of objective circumstances*. The focus is thus not on the details of individuals' lifestyles in the future but rather on the broad social circumstances that surround individuals. The subjective perceptions may reflect current developments and processes poorly but they give valuable insight into how individuals view the social world around them and its future. The images of the future of the participant clusters will be discussed in the next section.

6.2 Privacy Fundamentalists: The Drift to Low Privacy

Table 5 Privacy fundamentalists

Conception of privacy	*Threats*	*Responsibility*	*Solutions*	*Individual Control*
Right to be let alone and wide control over personal information. Functional for protecting the individual and maintaining intimate relationships.	Many threats: companies, governments, individuals	Individual	Personal coping strategies, personal responsibility. Anonymity. Raising awareness.	Illusory

6.2.1 Narrative

On the whole, the first cluster of participants had an attitude of uncertainty and anxiety towards the future of privacy. In 2050, privacy will be diminished through data collection and aggregation practices. An aggregated huge databank is currently only a matter of time and therefore it is likely to exist in 2050. This database will contain information on people's movements, shopping and leisure activities, among other things. The database will be run by a private company and it will sell people's information for profit. Surveillance will also be increased and new technologies such as minuscule microchips will enable surveillance in many surprising places. In terms of both data collection and surveillance, the individual has lost control over her privacy. A threshold has been crossed after which people can be read like an open book.

There were conflicting views on perceptions of privacy in the future. On the one hand, the general conception of privacy is unlikely to change radically and the majority of people will continue to regard privacy as important. On the level of values, then, people still consider privacy important. However, their actions together with the economic interests of companies lead to a gradual erosion of privacy. Young generations of the present lead the way by being increasingly individualistic and willing to expose themselves. They are fluent users of social media and they readily give up their privacy in return for benefits such as better services. This behaviour will increase in the future. As social media and digital communications technologies have become everyday phenomena, these services will no longer be viewed with suspicion.

Companies exploit the basic human need for communication as well as the new spirit of openness and sharing. People are made numb and lured with discounts and other benefits into accepting the increasing collection of personal data. Standards and norms change gradually: once people give more information, this becomes the standard and even more information is required in the future. There is thus an escalation of information collection. This process has already begun and there is no end in sight. People are not powerless but they do not see the gradual change process as a threat and they are lulled into a false sense of security and the illusion of control. Therefore privacy norms gradually drift towards less privacy protection. Privacy will become a commodity to be traded on the marketplace on a much larger scale than it is today, and those with less money will be particularly vulnerable to privacy violations. Gradually social control and lack of self-determination are seen as self-evident and desirable. This new low privacy world is coming and we cannot depart from this path. There will be even less individual control over privacy than there is at present. Invasions of privacy may stop when we feel that our most basic freedoms are invaded. It is only at this point that people may awaken to the aggregated loss of privacy, but it is uncertain whether control can be regained then.

6.2.2 Causal Layered Analysis

On the basis of the narrative and the privacy fundamentalist cluster's conception of privacy, the following CLA table was formed.

Table 6 CLA table: the drift to low privacy

Litany	***System/social causes***	***Discourse/worldview***	***Myth/metaphor***
Surveillance is an everyday phenomenon. Young people's behaviour leads to lower privacy standards.	Gradual systemic change. Slowly emerging data banks.	The tyranny of the normal. Active companies, passive individuals and governments.	Frog in boiling water. Crossing a threshold. The Cassandra myth. Individuals as driftwood.

Litany

The litany level of this image of the future does not necessarily seem threatening. On the surface level, privacy norms of individuals have changed and privacy, as it was understood before, is simply no longer desired. As an institution, privacy has become outdated due to new services that utilise new technologies. Surveillance, monitoring and data collection are everyday activities and they are not viewed as threatening and perhaps ignored altogether. However, from the perspective of the privacy fundamentalists, this development is threatening because people are not aware of the magnitude of the changes and of the importance of privacy as the right to be let alone and to control personal information.

At the litany level, privacy is at risk because young people share personal data without regard for consequences. Young people grow accustomed to such behaviour and thereby privacy within society as a whole is gradually eroded. The litany explanation for a drift to low privacy is that the behaviour of young people leads to diminishing privacy through changing social norms. One Israeli participant claimed that "young people are willing to expose themselves completely and they don't mind" (female, 61+ years).

System/social causes

In systems thinking, two central traps for systems are escalation and drift to low performance. Escalation refers to a situation familiar from warfare where actors continuously raise the stakes higher than their competitors, resulting in ultimately unsustainable exponential growth. Drift to low performance, in turn, means a situation where standards gradually fall because sub-average performance in the past is assessed as the standard level and goals are thus set lower, leading to an erosion of standards (Meadows, 2008, Chapter 5). I have chosen to call this image of the future 'drift to low privacy' because it resembles the situation of drift to low performance, although it has elements of escalation of privacy threats as well.

The mechanism of the drift to low privacy can be examined at the system level. The process can be illustrated with the following diagram.

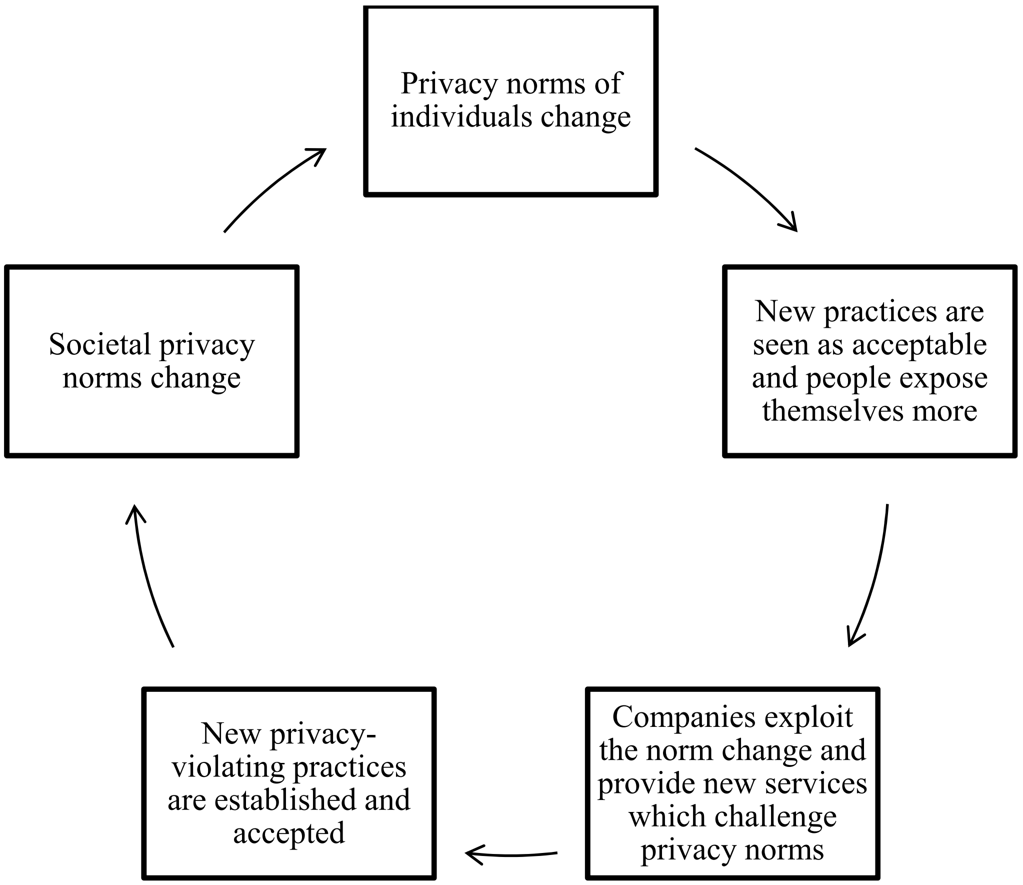
Privacy norms of individuals change
New practices are seen as acceptable and people expose themselves more
Companies exploit the norm change and provide new services which challenge privacy norms
New privacy-violating practices are established and accepted
Societal privacy norms change

Figure 8 Drift to low privacy

The diagram presents a cycle which leads to decreasing expectations of privacy and a decreasing overall level of privacy. The cycle in brief is the following. Companies create services which push privacy norms to become less strict. New privacy-violating practices are accepted and societal privacy norms change, which leads to new practices being accepted by individuals who internalise these norms. This creates demand for new services and companies then supply new services and the cycle continues. It is difficult to say where exactly the process begins, but it is reasonable to emphasise the role of companies because they are the active actor whereas individuals are seen to unthinkingly accept new practices. Therefore, the interests of companies can be seen as the driving force behind this development.

Warren and Brandeis wrote already in the 19th century that gossip journalism creates a vicious cycle where supply creates more demand, leading to the gradual lowering of social standards and morality (Warren & Brandeis, 1890, p. 196). The systemic causes for a drift to low privacy relate to such a vicious cycle or negative feedback loop. The process is comparable to environmental pollution. There is not one actor that is causing the erosion of privacy, but there are systemic effects that result from the interaction of countless actors which nevertheless lead in a clear direction. In the literature on privacy, Solove has recognised the parallel with pollution, claiming that in many cases of privacy problems there is no clear villain but privacy problems may emerge from activities that are not malignant as such, similarly to how pollution emerges due to industrial production. Furthermore, harms may build up from a gradual series of minor acts. According to Solove, many privacy issues “are systemic in nature” (Solove, 2008, pp. 177–178, 187). Nissenbaum also draws the analogy to pollution, stating that the aggregate of small privacy violations may add up to large harms beyond their immediate impact, in effect triggering a slippery slope into low privacy (Nissenbaum, 2010, pp. 242–243). Nissenbaum refers to insidious shifts in practice that are ultimately accepted as “the tyranny of the normal” (Nissenbaum, 2010, p. 160). In the drift to low privacy image of the future, privacy violations add up to systemic features, creating a threat that is more than the sum of its parts.

The drift to low privacy also relates to a kind of path dependency. As one focus group participant put it while discussing loss of control of private information: “We can’t divert from the path we walk on this regard” (male, 51–60 years, Israel). This means that past choices have led to a situation where future options are dramatically reduced. Such crucial choices could be for instance setting up of unregulated markets for personal information and low levels of privacy protection in popular social media services. Furthermore, the gradual build-up of data banks can be seen as a factor that leads to path dependency effects. Data is often collected in small amounts by various actors, but then it can be aggregated into a much larger data bank. Because of the nature of information networks, it is very difficult to remove data which has already been made public. Once the drift to low privacy has been set in motion, the system feeds itself.

Since the privacy fundamentalists viewed privacy predominantly as the right to be let alone and to form intimate relationships, these aspects will be at risk when privacy is diminished. One participant expressed the belief that if everything was public and privacy was lost, it would lead to chaos rather than openness (male, 21–30 years, Finland). This connection is interesting from the point of view of privacy as boundaries between normative circles. Loss of privacy would mean the erosion of boundaries, leading to a more chaotic situation where it is difficult to know who is entitled to what information and on what terms.

Discourse/worldview

The central discourse behind the drift to low privacy is the gradual shifting of what is viewed as normal, what Nissenbaum describes as “the tyranny of the normal” (2010, p. 160). The assumption is that people are extremely adaptable: they grow accustomed to even intolerable conditions if they are given time to adjust. In the Finnish focus group, there was discussion about an erosion of morality, and one participant expressed the threat of shifting standards in the following way: “the threat is that we begin to consider control as self-evident and even compatible with our own interest” (male, 21–30 years). The potential positive aspects of value change, such as transparency and openness, were not discussed.

Another discourse is the individualist and liberal notion of privacy. Privacy was seen an important but precarious right of individuals: the right to be let alone and to control personal information. Threats to privacy are seen to emerge potentially from many directions: from companies, the government, employers and unknown people on the internet (male, 21–30 years, Finland). This suggests a liberal interpretation of privacy as the protection of individuals against the government.

Even though the privacy fundamentalists were passionate about protecting their own privacy, the drift to low privacy image also includes a discourse of human passivity and fatalism. In its extreme version, the drift to low privacy is an image of the future where human agency has little possibility of affecting the future. It is as if the future emerges beyond our control, and we merely drift into this new era. The causal mechanisms are seen to be beyond the reach of individuals or groups of individuals. The drift to low privacy is therefore a somewhat fatalistic image of the future.

On the whole, companies with economic interests were seen to be the active actor in this image of the future. These actors and their interests are thus seen as the driving forces in change. In contrast, this cluster of participants viewed the opportunities of individuals, especially young people, ambivalently. On the one hand, they questioned the possibilities of individuals to control their privacy, especially in the future. Individuals are seen as passive recipients of services who are unaware of their privacy implications. On the other hand, the participants seemed to be exercising control in their own lives and they were suspicious about trading their privacy for material benefits. However, their actions could also be seen as coping strategies aimed at adapting to the new situation rather than being able to fundamentally change it.

It must be added that because control is seen as problematic, this does not mean that it is not seen as important. On the contrary, control seemed to be valued extremely highly by this cluster of participants, and this could be one reason for the scepticism about control. Because there is so much focus on control and very high expectations of control, it is seen as insufficient in the current situation. Participants within this cluster seemed to acknowledge that individual control is insufficient for guaranteeing privacy protection but they did not emphasise collective protection through legislation either. In addition, perhaps some of the privacy fundamentalists were conscious about being in a minority of privacy advocates whose opinions have little relevance for the future. One participant in the Finnish focus group was conscious about representing rather extreme views about privacy (male, 21–30 years).

The government as a potential protector of privacy is seen as a passive actor. One participant in this cluster stated that legislators cannot avoid dealing with privacy policies, but otherwise the government as an active agent was missing. Even the participant who mentioned the legislators considered that they will lag behind technological developments (male, 31–40 years, Germany). Privacy protection is mostly seen as the responsibility of individuals with limited control, and therefore the future of privacy can be seen as a dominating future in de Jouvenel's terminology.

A critical reading of the drift to low privacy image could see it as an alarmist scenario which aims at shock effect. Discussing alarmism in the context of infectious disease, Murray and Schwartz argue that alarmist accounts should be treated with the same critical outlook as overly optimistic ones, since individuals often have an incentive to overstate the gravity of problems to raise interest and gain media coverage. The authors also argue that pessimistic viewpoints are often accepted especially if they fit with an already prevailing pessimism within society (Murray & Schwartz, 1997, pp. 39–40). Applying this argument to discussions about privacy, there may be reasons to doubt at least the most radical alarmist accounts.

However, if the drift to low privacy is read as a conditional scenario of what could happen if nothing is done, the image is arguably more realistic. It is plausible that there could be a tipping point in the development of widely used technological systems and business models after which privacy is very difficult if not impossible to regain, for both individuals and societies as a whole. For individuals, it is difficult to unilaterally drop out of systems which are widely in use and have become part of the normal lifestyle, as Facebook and Google are currently becoming. This would at least involve great social sacrifices. On the macro level, in turn, if there is an economic ecosystem built around biotechnology, information technology and business models which utilise personal information, radically changing or abandoning these industries may become practically impossible. This is an example of path dependency which affects the future.

Furthermore, if privacy is seen as a collective good in Regan's terms and in this sense similar to clean air, for example, this has implications for the future. From this perspective, those who are not concerned about privacy and give up their privacy diminish the level of privacy for everybody else. For example, if camera phones are used by most people to take photos in public places, it is difficult for an individual to refuse having her photo taken. It can be argued that for the drift to low privacy to emerge, it is enough that a critical mass of individuals is unaware of privacy threats. In this sense, the privacy fundamentalists' fear of drift to low privacy is understandable.

Myth/metaphor

A fitting metaphor for the drift to low privacy is the image of the frog placed in cold water and ultimately boiled alive by gradually increasing the temperature. In a similar way, the drift to low privacy image of the future draws attention to a process of gradual change where there are no abrupt shifts and therefore the scope of the change is difficult to perceive. One Finnish participant spoke of a 'numbing' effect that continuous data collection has on people and of crossing a threshold after which privacy is lost (female, 31–40 years). Individuals become numb, like the frog in the boiling water, because they cannot see the slowly escalating societal impacts. In the drift to low privacy image, individuals are helpless and, like driftwood, they are moved by powerful currents.

It could be argued that this image of the future is a kind of tragedy where the individual as protagonist is set against companies and governments as the antagonist. Companies and governments see benefits in diminishing privacy and individuals short-sightedly sacrifice privacy for material benefits. The value of privacy is ignored by people who engage in hedonistic exposure until they realise that privacy is beyond saving. People willingly give up their control over privacy until they realise that it is impossible to regain control. The end state is life under constant surveillance and external control.

The Greek Cassandra myth also fits rather well with the ideal type of the privacy fundamentalist image of the future. Cassandra, the daughter of King Priam of Troy, had the gift of prophecy but she was also condemned in a way that no-one believed her prophecies. Her story then ended in tragedy because her true prophecies were not believed (Leeming, 2005a). The Cassandra metaphor has since been used in many contexts to refer to doomsayers. The Cassandra myth is apt for the drift to low privacy image of the future because in this image, a split is perceived between those who are aware of privacy threats and those who are not. In the extreme case, the one who argues for the loss of privacy views herself as the only one who realises the threat to privacy, while others are unaware and do not believe her which leads to the drift to low privacy. The extreme version of this notion is of course implausible. If the privacy fundamentalist is aware of threats to privacy, why are others not aware? Why are others operating under false consciousness while the Cassandra is not?

6.2.3 Discussion: Problems and Solutions

On the system level, the crucial issue in the drift to low privacy image is that no balancing feedback loop is conceived to stop the drift. Meadows argues that solutions to escalation and drift to low performance are the following: refuse to compete or create a new system with balancing loops, or keep performance standards absolute (2008, Chapter 5). One systemic solution to a drift to low privacy could be to maintain an absolute value and definition of privacy in the face of threats. Strict privacy legislation could be passed as a solution to eroding privacy norms. However, such a rigid conception may not be helpful if individuals are not committed to it. Refusing to compete and creating a new system are also possible solutions, but one could ask if it is possible to simply drop out of all the systems that currently threaten privacy. For example, in a society that uses Facebook for many communication needs, dropping out of the system may entail great social sacrifices. Creating a new system altogether is also a rather utopian solution.

As a first step, increasing awareness and educating people about the threats to privacy could lead to the creation of a balancing feedback loop. An Israeli focus group participant stated about the new technological world: “It’s going to happen anyway, so let’s go there with our eyes open” (female, 31–40 years). More education would lead to a situation where individuals have better intellectual resources to claim their privacy. In particular, knowledge about the wide-ranging impacts of actions is crucial for preventing the drift to low privacy. A related solution was raised by one Finnish participant: dialogue and discussion (male, 21–30 years). At best, dialogue can respect individuals and incorporate multiple individual points of view while engaging with others. However, it can be argued that individuals alone cannot protect their privacy against systemic threats even if they are aware of the threats. In addition, there will always be individuals who are not fully aware of risks. Therefore, collective privacy protection is also needed to avoid the drift to low privacy.

On the metaphor level, the solution was already hinted at. The drift to low privacy should not be interpreted tragically as an inevitable scenario. Instead, it should be seen as a primary forecast in de Jouvenel’s terms, that is, a story of what happens if nothing is done (de Jouvenel, 1967, p. 55). In this interpretation, the current passivity of individuals is changeable rather than being an existential condition of life.

6.3 Privacy Pragmatists: Continuity and Benign Evolution

Table 7 Privacy pragmatists

Conception of privacy	***Threats***	***Responsibility***	***Solutions***	***Individual Control***
Privacy is a shared value. Privacy is important but not extremely serious.	Traditional threats such as criminals.	Both individual and collective	Common sense, traditional mechanisms.	Real

6.3.1 Narrative

The second cluster of participants, the privacy pragmatists, had a less clear image of the future than the first cluster. On the one hand, the perception of privacy will be different in the future, and discussions of privacy in the early 21st century will seem antiquated in 2050. New communications technologies will bring people closer to each other regardless of location, and in this sense the world will become smaller. There are also threats to privacy from criminals and hackers, for instance. On the other hand, privacy as an institution is not in great danger. Privacy has a long tradition and it has been similar for a long time. Privacy will remain important and in the most fundamental aspects of life it will remain similar to today, but it is difficult to say exactly how privacy will be perceived in the future. The threat of losing one's privacy will also remain an important concern and awareness of this threat will lead to people holding onto it more tightly. In this way, people will not let the threats materialise. In many cases, common-sense precautions and traditional protection means such as consent and professional confidentiality are enough to protect privacy. There will thus be changes in the perception of privacy but these changes are not particularly threatening and privacy will remain an important institution and aspect of life.

6.3.2 Causal Layered Analysis

On the basis of the narrative and the privacy pragmatists' conception of privacy, the following CLA table was formed.

Table 8 CLA table: continuity and benign evolution

Litany	***System/social causes***	***Discourse/worldview***	***Myth/metaphor***
Privacy will remain important but it will be perceived differently.	Privacy is in equilibrium. There are no systemic threats.	Pragmatism and balance: there are two sides to negotiating privacy.	Stability and slow evolution. Business as usual and continued manageable growth. Pax Romana. Plus ça change, plus c'est la même chose. The flowing river and the stable riverbed.

Litany

On the litany level, the privacy pragmatists represent so-called ordinary people. If asked about privacy, they view privacy as important but it is not their first priority and it is difficult to express why privacy is important. Correspondingly, their image of the future was rather pragmatic and intuitively 'realistic' although rather empty of substantive content. It seems common sense that perceptions of privacy will change due to new technologies, among other things, but that privacy will remain an aspect of life that individuals want to protect. Since the privacy pragmatists present such a pragmatic image of the future and understanding of privacy, these are difficult to criticise on the litany level.

System/social causes

The privacy pragmatists viewed traditional methods of privacy protection as largely sufficient. These include requiring consent when giving information and professional confidentiality and only using information for the purposes for which it is collected. However, the participants emphasised that there need to be real consequences from breach of confidentiality and that consent needs to also work in practice. Concerning the individual protecting her own privacy, the pragmatists also mentioned personal coping tactics such as not spreading personal things and leaving one's address out of the telephone directory. In other words, common sense and traditional mechanisms are seen to protect privacy quite well.

It could be argued that the privacy pragmatists view privacy within society in a kind of state of equilibrium. There are no great systemic challenges to current privacy norms, and if a threat emerges, individuals or the state can manage it and no radical corrective movements are needed. The main threats were seen to come from criminals engaging in identity theft, for example. In general, the privacy pragmatists considered individuals as active and they were optimistic about their possibilities of controlling their privacy.

The pragmatist image of the future can be seen as the mirror image of the drift to low privacy image. In a sense, privacy pragmatists are exactly the people that are believed to enable the drift to low privacy, according to the privacy fundamentalists. If we believe, as the pragmatists do, that privacy is not under particular threat, what could stop the drift to low privacy, if such a process were actually ongoing? From the privacy fundamentalist perspective, it is more reasonable to be alert than unaware because the risks of false alarmism are in any case smaller than the risks of being unaware.

Discourse/worldview

Participants in this cluster tended to be rather pragmatic on privacy issues. Privacy was seen as an important value but not the most important priority. As one participant put it in the context of data protection, “we shouldn’t get hysterical” (male, 51–60 years, Finland). Participants emphasised balance and the fact that there are two sides to negotiating privacy. On the one hand, there are concerns over one’s profile being in many places but on the other hand, one can also benefit from improved services by giving information (male, 51–60 years, Finland). This balance also applied to the perceived nature of humans: humans are social animals but we also need our own nest where we are sometimes let alone (male, 51–60 years, Finland). On the one hand, we live together in society and personal information is not private property, but on the other hand, privacy can be negotiated and traded if the benefits are sufficiently attractive. Likewise, the protection of privacy should be a combination of individual and government efforts.

One participant considered that identity is a means of trade and that we have no choice on the matter, but on the other hand, she is quite similar to other people in her age group and therefore she is not concerned about her privacy (female, 51–60 years, Finland). This is an example of the protection by obscurity argument that was discussed before. It is also an example of the arguments of balance that participants in this cluster tended to promote.

It could be that privacy pragmatists considered different aspects of privacy than the privacy fundamentalists, for example. If privacy is seen as physical integrity and safety within one’s home, for example, then it is likely that privacy is more stable than if one considers personal information. The integrity of the home was emphasised by some participants in this cluster. However, trading with personal information was also viewed in a rather pragmatic way. Another argument could be that because privacy pragmatists view both individuals and the state as active protectors of privacy, they see no serious and unsolvable threats to privacy.

Myth/metaphor

The pragmatist image of the future can be connected to an underlying conception of stability and evolutionary change, that is, a view of the future as 'business as usual'. As Schwartz (1996, pp. 147–148) notes, evolution implies slow change which is easy to manage. This is close to the archetypical 'continued growth' image of the future which James Dator (1979) has identified, although the image also includes aspects of Dator's 'disciplined future' image. Inayatullah argues that the image of continued growth makes sense for individuals because it posits a safe vision of the continuity of present processes (1993, p. 243). It must be added that in the pragmatist image of the future, present processes are not seen as threatening.

A metaphor for this conception could be the Pax Romana, the long period of peace during the first and second centuries AD. Another suitable metaphor is the flowing river and the stable riverbed. There is also a proverb which describes the pragmatic attitude quite well. In the original French, it is "plus ça change, plus c'est la même chose" and it is often translated as "the more things change, the more they remain the same". The underlying notion is that changes are only superficial and the deeper structures remain the same. The surface of the river changes constantly but the riverbed is much more stable. These metaphors capture the conservatism inherent in the pragmatist position. In a sense, this conception is similar to the layered approaches of causal layered analysis and ontological critical realism, where surface phenomena are underpinned by a more stable foundation of causal mechanisms and cultural myths, respectively. However, both Inayatullah and the critical realists acknowledge that deeper changes are also possible.

6.3.3 Discussion: Problems and Solutions

On the surface level, the image of continuity and slow evolution seems plausible and perhaps also desirable. If the image itself is assumed to be plausible, the only immediate disadvantage of such development is the lack of radical innovations and improvements. However, in futures studies the assumption often is that if anything, change will become more rapid in the future and that the future is usually surprising in at least some ways. For instance, Anita Rubin has noted that the images of the future of teachers are based on the assumptions that the institutions of the industrial society will persist and that development will continue in the same direction as it has in the past. The problem with this type of thinking is that it may be unsustainable when new phenomena such as radical technological innovations constantly challenge these institutions (Rubin, 2013, pp. S42–S43). For Bell (1997, pp. 141–142), one of the key assumptions of futures studies is that the future will contain features that are not familiar from the past and the present.

From this perspective, an image of the future may seem plausible because it is at the moment the culturally predominant way of seeing the future. Of course, this alone does not mean that it is a particularly probable future. A plausible image of the future may be a comfortable view of the future which avoids the cognitive dissonance associated with thinking about radical changes (Inayatullah, 1999, p. 53). This image of the future should be contrasted with other approaches and with knowledge of potential threats to privacy. It should be asked whether there actually are serious privacy threats, as many contemporary commentators argue (e.g. Froomkin, 2000; Nissenbaum, 2010; Solove, 2008). If it can be plausibly asserted that there are no serious threats to privacy, then a pragmatic view is the most sensible one. However, if there are real threats and risks, then denying them could be likened to climate change denial where a process which is widely seen as real is not considered real because it is not immediately visible and because there are also counter-trends.

In addition, the conception of social change as slow, manageable evolution with stable underlying structures should be questioned. In fact, even evolutionary futures studies emphasises periodical step-wise shifts that divide societal development into periods which can be given labels such as the industrial age and the information age (Mannermaa, 2007, pp. 108–109). The privacy pragmatists' conception of stable, slow evolution focuses only on the relatively stable periods between these shifts and ignores abrupt changes or paradigm shifts. The pragmatists overemphasise the riverbed at the expense of the flowing river. Schwartz (1996, pp. 159–160) warns against scenario plots with an unbroken line. Trends of continuous growth tend to decelerate or change direction at some point in the future.

6.4 Privacy Individualists: Privatised Privacy and an Uncertain Future

Table 9 Privacy individualists

Conception of privacy	*Threats*	*Responsibility*	*Solutions*	*Individual Control*
Different things for different people. Privacy can be controlled, negotiated and traded with. Functional for protecting the intimate sphere.	New technologies. Government is a more serious threat than business.	Individual	Common sense, personal responsibility. Obscurity.	Real

6.4.1 Narrative

The privacy individualists saw the future as unknowable. They considered it likely that there will be significant changes in lifestyle by 2050. Technological progress is the central driving force behind these changes. Because of technological progress, privacy will certainly be different in the future. Technological systems and practices such as the intelligent networked home, money on a chip implanted in our neck, a sensor inside our head and surveillance of our home could be in use. Legislation will always lag years behind such technological developments. In the market for personal information, the supply and demand will meet each other and there will be a price for privacy, and there will be more government surveillance, whatever kind of government there will be at that time. There is also the danger of classification of individuals by the state. So far, we have only seen the beginning of this process.

Because of the rapidity of the change, the future is very uncertain and it is difficult to know much about the future. Privacy will remain important but the circumstances will be different and people are likely to share their information more liberally. Since privacy is a changing phenomenon, the foundations of privacy have to be continuously translated and accustomed to new situations. Hopefully one's thoughts will remain private even if one's home will not. There will be increasing emphasis on the individual's own control over her own privacy.

6.4.2 Causal Layered Analysis

Based on the narrative and the privacy individualists' conception of privacy, the following CLA table was composed.

Table 10 CLA table: privatised privacy

Litany	***System/social causes***	***Discourse/worldview***	***Myth/metaphor***
Technological progress is unstoppable and the definition of privacy must be translated to new circumstances. Individuals freely trade with their privacy.	Technological development and the free market of information produce unforeseeable results.	Individualism, liberalism. The independent individual standing against society.	The Prometheus myth. The lone ranger. David versus Goliath. The stormy ocean.

Litany

Technology is seen as the main driving force behind developments. Technological progress is seen as an unstoppable force that changes lifestyles, and privacy will have to be adapted to the new technological surroundings. Technology thus ultimately determines the possibilities of privacy but individuals can manage their privacy within the limits set by technology. Privacy is not completely lost but it is radically reconfigured, most likely into a free market of personal information. Therefore, individuals can freely trade with their privacy which has effectively become a commodity. Each individual is responsible for protecting her own privacy using whichever means she has at her disposal.

System/social causes

From a systemic perspective, the individualist notion of privacy is linked to an unforeseeable future because many technological developments are seen to interact on the free market. The protection of privacy is not coordinated by any actor and it is the responsibility of individuals to protect their own privacy whichever way they can. The individualist conception of privacy arguably leads to some systemic risks. Since privacy is approached from the individual point of view, privacy protection is not viewed holistically, and therefore unplanned social change can lead to undesirable results for everyone. At worst, this can lead to a chaotic future where tensions are mounting but there are no mechanisms for controlling them. No-one is responsible for the big picture and individuals can only find coping strategies in this situation. On the other hand, if one believes that a lack of centralised control will produce a dynamic equilibrium, the situation can be seen as very efficient because there is no legislation to slow down the development of technological innovations.

Legislation was viewed as slow and passive by the privacy individualists. They considered that legislation always lags behind technology. The assumption is that market-driven technological advances develop faster and more flexibly than legislation which is created through a relatively slow process. The discourse connected to this explanation is that markets are efficient and proactive and that legislation is essentially reactive. Moreover, the discourse is that this is a natural feature of these systems, that is, that technology will by necessity outrun legislation. It could be argued that in this liberal view, technology or the market mechanism are seen as the drivers of social change and legislation only has a guiding or restricting role.

It depends on one’s ideology whether legislation lagging behind technological developments is viewed as a problem. From a liberal perspective, the situation that legislation lags behind technology is normal and positive. From this perspective, the role of the government is not to guide social and technological developments but to give the freedom to private companies and individuals to pursue their own ends. If problems do occur, governments can then reactively press for legislation to mend the situation. In contrast, from a social democratic perspective, the state should proactively shape social development towards democratically chosen goals.

Discourse/worldview

The worldview of the individualist image of privacy is that of individualist liberalism. One is allowed to pursue one’s own projects and to pursue happiness in one’s own way as long as no harm is done to others. A liberal discourse is very prominent within privacy theorising. Fuchs goes so far as to claim that there is a “liberal bias” in the concept of privacy itself and that the modern privacy concept is inherently connected to liberal thought (2011, pp. 220, 223). The privacy individualists expressed this perspective the most clearly compared to the other clusters of participants. The fear of categorisation by the state is clearly connected with a liberal outlook.

Participants in this cluster were also the closest to technological determinism among the participants. David Brin expresses the technological determinist view well: “No matter how many laws are passed, it will prove quite impossible to legislate away the new tools and databases. They are here to stay” (1998, pp. 8–9). From this perspective, technology is an independent actor which cannot be controlled by other actors. It is an independent variable rather than a dependent one. There is some truth to this due to path dependency caused by technology, as was already argued, but from the critical realist perspective, for example, it is unjustified to view technology as an independent social agent.

The privacy individualists viewed privacy as a commodity that can be traded by individuals for benefits. Some commentators argue that privacy should indeed be viewed as private property. It has been argued that giving individuals a property interest in their personal information would lead to them having more control over their information. The argument is that if people view their information as property, they can bargain with it and exchange it for other goods in the market (Tavani, 2008, p. 134). However, others criticise this development because it privatises the social phenomenon of privacy and neglects the public and collective value of privacy.

The central discourse of the privacy individualists is the independent individual who is separate from society and stands against society. Privacy is viewed as the protection of this individual against the state and other public actors. This view is partly truthful in the light of the historical emergence of privacy together with individualism, as Schoeman has emphasised (1992, pp. 113–114). However, this approach ignores the nature of privacy as a social institution, as a *social* form of protection of individuals. Since privacy is viewed only from the individual's perspective, the future of privacy is more difficult to imagine than the future of privacy as a social institution. In the ideal-typical form of the individualist discourse, individuals are required to stand alone against society. One issue, then, is the protection of those who are for some reason less capable of protecting their own privacy, such as children and people with low income.

Myth/metaphor

The individualist image of the future can be connected with two central metaphorical aspects: the myth of Prometheus, on the one hand, and the lone ranger, on the other hand. The myth of Prometheus describes technological progress through the application of knowledge and science. In Greek mythology, Prometheus was a Titan who angered the high god Zeus by stealing fire to humans from the gods and teaching arts and survival techniques to humans. As a punishment, Prometheus was bound to a rock and tormented (Leeming, 2005b). The Prometheus myth can be seen as a metaphor for humans gaining control over their environment through knowledge and technology. As Heinonen notes, the Prometheus myth is problematic because it can lead to hubris. From the ecological perspective, the Promethean view of technology could lead to humans considering themselves as something above nature, to irresponsible use of technology and ultimately to ecological or genetic catastrophe (Heinonen, 2000, pp. 193–202). In the privacy context, it could lead to an irreversible loss of privacy due to technological lock-in. This dual nature is also apparent in the individualist image of the future of privacy. On the one hand, individuals can freely trade with their privacy, but on the other hand, uncontrollable technological progress could ultimately endanger their privacy. Using a water metaphor as in the previous images, the future can be seen as an uncontrollable stormy ocean where each individual navigates to the best of her abilities.

In addition, the liberal notion of the independent individual standing against society can be connected to the mythical figure of the lone ranger or the solitary hero. In the lone ranger narrative, the heroic individual confronts an oppressive social environment and prevails over the impersonal system. The battle between David and Goliath is one example of this narrative. My argument is that the privacy individualists view themselves as kind of lone rangers who need privacy in order to defend themselves against society. Crucially, the lone ranger is a hero who is capable of individually protecting her privacy. The lone ranger myth, while powerful, can also be harmful because it leaves individuals to pursue their private victories alone, and it can also create conflicts when two or more lone rangers interact (Schwartz, 1996, pp. 155–156). There is also a similar problem of dichotomy as in the Cassandra myth of the privacy fundamentalists: is it plausible to claim that the privacy individualist is the exceptional lone ranger while others are part of an impersonal system?

6.4.3 Discussion: Problems and Solutions

The main problem with the individualist image of the future is that the future is seen as radically uncertain and uncontrollable. Solutions to privacy problems in the individualist discourse tend to be connected to the activities of individuals and they can be seen to remain on the litany level. These solutions can best be described as tactics for coping with privacy threats. The benefit of such solutions is that they are immediately implementable: one does not have to rely on uncertain political or legislative processes. Their weakness is that they are only short-term solutions and they do not address the roots of problems or systemic risks. In this sense, the privacy individualists are similar to the privacy fundamentalists. In de Jouvenel's terms, the future of privacy is seen as a dominating future. However, the two images of the future view different actors as active. For the privacy fundamentalists, the actors are mainly companies with economic interest, for the privacy individualists, technology is an actor.

The view of legislation lagging behind technology could be countered with the possibility of proactive legislation. Legislators could use foresight to proactively tackle future challenges or at least be prepared for them. In addition, it could be argued that legislation also has a constitutive role: it creates the frameworks within which commercial and technological players act. Without the institutional frameworks such as higher education and protection of intellectual property, developing technology could in effect be impossible. It is widely accepted today that fostering innovations requires an innovation system. Therefore, it could be argued, contrary to the notion of technology outrunning legislation, that the development of technology is itself contingent on social factors such as legal frameworks and institutions (Edge, 1995). Thus the relationship of technology and legislation is more complex than the individualist view suggests. This kind of systemic view of technology and legislation would lead to a different litany than the one of privacy legislation always lagging behind technology.

6.5 Privacy Collectivists: A Responsible Future or Moral Decline

Table 11 Privacy collectivists

Conception of privacy	***Threats***	***Responsibility***	***Solutions***	***Individual Control***
Control over information and access but also a shared, public and collective value. Functional for maintaining autonomy and democracy.	Lack of awareness, knowledge and transparency are the main threats. Companies, governments.	Collective	Broad regulatory framework. Raising awareness.	Real

6.5.1 Narrative

The attitude towards the future of the fourth cluster, the privacy collectivists, can be briefly described as deontic. In other words, the future of privacy is seen from the perspective of duties and obligations. The future depends on the model that current generations set for future generations. If privacy is respected, it will remain as an eternally important value in a changing technological environment and its function of enabling self-determination will not change. The involuntary use of personal data will continue to be debated in the future. There are government regulations in place for banning the free trade of personal information and for regulating people’s exposure. The government also provides information about privacy so that individuals can make informed choices about sharing their information. As a result, citizens are protected against inequality and discrimination. The private sphere is protected by regulations so that citizens can come together as equals in the public sphere. This is the positive image of the future of this cluster.

On the other hand, there are two negative images of the future. The first one relates to an internal threat. If people continue to engage in overt communication about their private matters which disregards the value of privacy and does not fit human nature, this leads to a great catastrophe and the collapse of society as a moral community. Since humans are dependent on each other for recognition and for building their social identities, complete exposure will change their self-image. The second negative image relates to an external threat to privacy. Privacy as a shared value may be sacrificed in the race for information between governments and business. A disregard for the value of privacy from these institutions leads to an escalation of privacy-violating practices. Because privacy as a shared value is a crucial foundation for democracy, both negative images place the future of democracy at risk. Furthermore, because privacy is a collective value, the downgrading of privacy by some will cause loss of privacy for all.

6.5.2 Causal Layered Analysis

Based on the narrative and the privacy collectivists' conception of privacy, the following CLA table was composed.

Table 12 CLA table: responsible future or moral decline

Litany	***System/social causes***	***Discourse/worldview***	***Myth/metaphor***
Privacy is a social value which promotes autonomy and which must be protected by legislation. If privacy is protected, the future is stable. If it is not protected, there will be a moral decline.	Balance: Privacy maintains democracy by enabling the formation of the public, and democracy maintains privacy.	Social democracy or communitarianism. Society as a moral community. Collective protection of important values.	Stable, disciplined future. Challenge and response. The dammed river.

Litany

The litany view of this image of the future is that privacy is a crucially important shared value which enables self-determination and democracy and therefore it is likely to be protected. There are risks to privacy from both businesses and government, and therefore legislation needs to be constantly updated to protect privacy. At litany level, the image is otherwise not problematic. Democratic nation-states protect privacy through legislation, which helps to maintain individual autonomy and the value of privacy. The positive image of the future of this cluster is rather close to a utopia and the negative images have a dystopian quality.

System/social causes

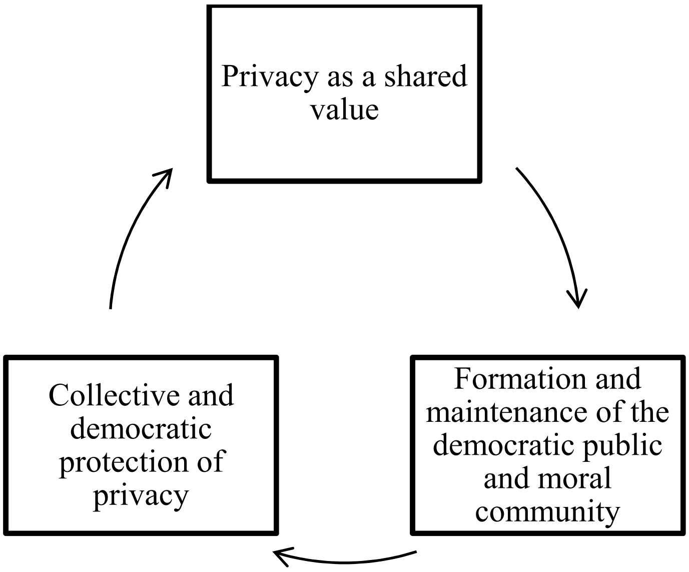
Privacy as a shared value
Formation and maintenance of the democratic public and moral community
Collective and democratic protection of privacy

Figure 9 Collective protection of privacy

Crucially, the cycle presented by the privacy collectivists is a maintaining one rather than a cycle of exponential growth. If privacy remains as a shared value, this enables the formation and maintenance of the democratic public, which then collectively protects privacy through the political process. Privacy is protected by regulating exposure and trade of information and by giving information about privacy, which in turn maintains privacy as a shared value. There is thus a virtuous cycle that maintains democracy and welfare. However, extrinsic influences may break the cycle. Such influences could be companies with an interest in collecting information or excessive governmental control and scrutiny. If privacy is no longer viewed as a shared public value, that is, if the normative circle around privacy norms breaks into many normative circles with their own notions of privacy, then the equal democratic public and collective protection of privacy may be questioned. One plausible scenario would be that citizens' trust in the government diminishes for some reason and as a result the government is no longer seen as a reliable protector of privacy. Then the situation would become similar to the individualist view of the future of privacy. The result is the formation of smaller normative circles or, at worst, anomie and normlessness. The collectivist image of the future is thus contingent on maintaining society as a unified moral community, the possibility of which can reasonably be questioned in the present social circumstances.

In this image of the future, the government is seen as an active agent. Correspondingly, individuals are seen as less active, and they are largely active through the political process. This leaves less space for individual strategies of protecting privacy. Within this cluster, technology was not viewed as a major threat to privacy. One participant explicitly expressed a neutral view of technology, stating that it does not matter which tool is used to publish personal data as long as it is done knowingly and voluntarily (female, 21–30 years, Germany). Companies and governments were also seen as potential privacy threats but the threats posed by them were not emphasised.

Discourse/worldview

The central discourse behind this image of the future is a view of society as a moral community, which must be an imagined community since to a large extent its members are not directly interacting with each other. The ideology behind this image of the future includes elements of communitarianism, social democracy, human rights and an attitude of responsibility towards the future. The future is described more as a desirable or undesirable future than a probable future. I would argue that this is why in this cluster there were different images of the future. From this perspective, the future is seen as heavily contingent on human behaviour rather than being determined by technological development.

In accordance with the communitarian discourse on positive rights, privacy is not only seen as the right to be let alone but also the right to autonomy and to shape society. In this ideology, the freedom of humans is not challenged by the active agency of the government, because unlike in classical liberalism, the individual and society are not seen as conflicting forces but rather society consists of individuals and the society or community, in turn, has an active role in shaping individuals.

One Israeli participant promoted an egalitarian privacy ideal: “Privacy must be uniform: everybody must be exposed or concealed in the same amount” (female, 21–30 years). This position could be described as egalitarian and social democratic. This egalitarian ideal is this image’s main strength and weakness. On the one hand, centrally regulated privacy protection acknowledges the value of privacy and does not make it the responsibility of individuals experiencing harms to seek justice through lawsuits, as is the case in a more individualist model (Dawes, 2011, p. 120). In this way, even those who are unable to protect their privacy by engaging in lawsuits can have privacy.

Myth/metaphor

The collectivist image of the future can be connected to Dator's 'disciplined society' image (Dator, 1979). In this archetypical image, the future is collectively controlled and there are mechanisms for managing the risks of technological development. If this collective control fails, then the image changes to a negative image of collapse. This image of the future is thus a kind of conditional image which includes two possibilities depending on whether the community passes the test of protecting privacy.

Therefore, the collectivist image can also be seen as a "challenge and response" type of narrative where the community continually faces challenges relating to privacy protection, but these challenges are tackled by collective action and the political process (Schwartz, 1996, pp. 144–147). Using a water metaphor, like in the previous images of the future, the responsible future can be seen as a dammed river, controlled and harnessed to serve human goals. Among the images of the future, the positive collectivist image was the closest to a utopian image. While such utopian images can serve as inspiring visions, their assumptions must also be compared with knowledge about the barriers to change, what Inayatullah (2008, p. 8) calls the weight of history and what were earlier (section 2.1) referred to as the ongoing processes which make certain futures much more likely than others. It could be argued that such barriers exist both subjectively, in the consciousness of actors, and objectively, as features of society. These are factors which limit the openness of the future.

6.5.3 Discussion: Problems and Solutions

The litany-level solution to the problems identified in this image would be to increase awareness about privacy as a value to ensure the commitment of individuals. The corresponding social solution would be to include discussions of privacy within the curricula of schools, for example. Privacy could be taught as a central value alongside other societal values such as equality and liberty. Another system-level solution would be to legally guarantee a minimum level of privacy.

However, these solutions address only the surface issues. On the deeper level, a solution must be found to the paradox of protection of many different normative circles by a central power. A solution should be found where there is wide consensus on the *value* of privacy and the need for regulative protection, while there is also a respect for the contextuality of privacy norms and the diversity of opinion on the topic. One solution could be DeCew's (1997, pp. 161–162) approach of dynamic negotiation which states that there should be a presumption in favour of privacy but individuals can opt for less privacy if they wish to do so. This presumption in favour of privacy could be legislated but informed individuals could choose to have less privacy.

One participant in this cluster argued for our responsibility to future generations, that we should keep future generations in mind when balancing privacy with other interests such as economic interests: "If we make this possible now, what will happen to our children?" (female, 31–40 years, Finland). A responsible attitude towards the future is a sensible first step in a solution to privacy issues. The narrative of challenge and response is fitting for this attitude.

However, the metaphor of a disciplined society is more problematic. The ideal of collectively managing societal problems gives the collectivist image of the future a utopian character, as was already mentioned. The image assumes that there is substantial consensus on values and ignores the many value conflicts that are part of contemporary society. Similarly, changes in privacy are conceived only in terms of collectively maintaining shared values or moral collapse. There is thus no conception of the contextuality of privacy or changes in privacy that would not lead to moral collapse.

One potential problem with the egalitarian approach to privacy is that in aiming for a common level of privacy protection and a regulated divide between public and private, it neglects the individual experiences of privacy which are in a sense at the core of privacy protection. There is the danger of reifying the concept of privacy and the public/private divide in the face of continuous technological progress, social mobility and social fragmentation which challenge such rigid definitions.

Furthermore, the discourse of society as a moral community is problematic at present because the borders of such communities are increasingly blurred. The nation-state, for instance, is no longer an obvious source of social identity for individuals. Indeed, as was argued in discussing the definition of privacy, normative intersectionality is presently the normal situation. This is most evident in multicultural societies where norms about privacy and many other issues differ across ethnic groups. Even in ethnically homogeneous societies there are different worldviews and outlooks. Moreover, geographical mobility has increased in recent decades, which suggests that social fragmentation will tend to increase rather than decrease. Mobility and globalisation present challenges to legislation. If privacy threats are global, would regulation also need to be global?

There are also some ethical problems with the notion of a unified moral community. This notion makes privacy norms appear as consensual and it can hide conflicts and power relations. If comprehensive privacy norms are legislated by majoritarian democratic system, there may be a substantive minority who do not agree with the norms. In this case, the majority uses political power to impose its definition of privacy. The collectivist image thus presumes a wide consensus on the scope of privacy. Moreover, if privacy is seen as the institution maintaining boundaries between norm circles to protect from central power, does the moral community approach undermine privacy and promote a single ‘public’ rather than a society consisting of many normative circles? By protecting a democratically agreed definition of privacy, the social freedom of individuals may undermine individuals’ social freedom.

The crucial challenge for the collectivist image of the future is whether it is possible and desirable to collectively protect shared privacy norms in a situation where society is formed of multiple groups rather than a homogeneous public. This is the image of intersecting normative circles which was referred to earlier. This challenge touches on the problem raised in the theoretical section, that privacy norms of normative circles must be respected by actors outside that particular circle. If there was a homogeneous public that constituted one normative circle with similar privacy norms, protection of privacy would be unproblematic. On the other hand, taken to the extreme, such a situation would mean that there is only one normative circle and privacy would mean protection of the integrity of individuals within this circle rather than protection of the integrity of many circles where individuals can participate. There is a kind of paradoxical situation here: privacy is seen as best protected by a central power but the function of privacy is to protect spheres of life from a central power.

6.6 Discussion of the Privacy Conceptions and Images of the Future

Each image of the future has its own virtues which are connected to the underlying assumptions about privacy and about aspects affecting it. The privacy collectivists, for instance, are right in claiming that individuals alone cannot protect their privacy when there are systemic threats to privacy. The future of privacy is largely a dominating future if individuals are seen as the only protectors of privacy. The social value of privacy is also clearly seen by most privacy collectivists. On the other hand, the privacy fundamentalists are correct in emphasising that privacy will not be protected if individuals are not interested in their privacy. Collective protection such as legislation will have little influence if individuals voluntarily give up their privacy. The fundamentalists are also right to argue that individuals should have real control and awareness concerning privacy, not only formal consent and illusionary control.

Privacy individualists, in turn, make a valuable point in emphasising that in reality individuals are active and exercise control in many ways, including sometimes trading with their privacy. They also rightly highlight the effect that new technological systems are likely to have on privacy. Finally, the privacy pragmatists bring a balanced view to the discussion by seeing privacy as an important aspect of life but not the highest priority. There are always many sides in discussing privacy, and more privacy is not necessarily better in each context.

On the other hand, each image of the future has its weaknesses. The privacy fundamentalists tend to underestimate the agency of individuals and the ability of decision-makers to create privacy legislation if privacy is felt to be under threat. The privacy individualists, in turn, tend to overstate the possibility of individual control while perhaps acknowledging that control may be at risk in the future. In addition, they ignore the protection of those unable to protect themselves. Privacy pragmatists have no clear image of the future which may lead to an attitude of passivity. They tend to rely on the continuity of present developments which are not seen as threatening. Finally, privacy collectivists do not consider the challenges to centralised privacy legislation, such as social fragmentation, which put the notion of 'the public' and privacy as a shared value at risk. In general, it could be stated the individualistic images of the fundamentalists and individualists tended to have an attitude of fatalism or determinism from the individual's perspective. Either powerful companies or technological progress determine the path to the future and most individuals are left with little agency or choice. In both of these images, individuals have to cope in the new reality because they cannot change it, although the privacy individualists are more optimistic about individuals' possibilities of controlling their privacy. The more collectivistic images of the pragmatists and collectivists, in turn, tend to be more optimistic and closer to utopianism, in the form of a stable future or a disciplined future that is controlled collectively.

Perhaps it is useful to view the alternative images of the future as different kinds of forecasts. In de Jouvenel's (1967, p. 55) terms, forecasts can be primary, secondary or tertiary (historical). The drift to low privacy is a primary forecast: this is what happens if nothing is done. The positive version of the collectivist image of the future is a secondary forecast: this is what happens if we collectively continue to uphold privacy as a value. The pragmatist and individualist images of the future, in turn, are attempts at historical forecasts: in reality, we do not know how different actors will behave. Therefore the future is uncertain and can be seen as either stable or turbulent.

The first step in a solution to privacy problems is an attitude of *responsibility* for the future or caring about the future. For Adam and Groves (2007, Chapter 9), caring about the future means reconnecting action, knowledge and ethics. This attitude entails recognising processes that are already in motion and recognising path dependency. In other words, the future implications of present action should be acknowledged.

I would argue that the main conceptual challenges in privacy protection stem from the contradictory nature of privacy. Privacy is contextual and universal at the same time. It is seen as relative and traded for many benefits in practice at the same time as it is elevated as an absolute value. It is an everyday phenomenon to which we do not devote much thought but it is also seen as a necessity for civilised life. Within this study, this dual nature of privacy was apparent both in the theoretical literature and in the focus group discussions. In my view, the academic literature on privacy cannot avoid engaging with the normative evaluation of privacy. An attempt at a purely descriptive account would still have a relation to normative accounts because it would need to argue against them. As Nissenbaum (2010, pp. 3, 10) notes, privacy theories generally tend to discuss privacy either as an intrinsic value or as an interest to be balanced with other interests. Thus privacy is either elevated or lowered.

In my view, Schoeman, Nissenbaum, Solove and others are correct in discussing privacy in relation to social norms as opposed to interests or ultimate values. However, Nissenbaum's own account limits the value of privacy to maintaining existing contexts and in this way it again lowers privacy. I would argue that Schoeman comes closer to a suitable account of privacy with his theory of social freedom and the integrity of spheres of life. Privacy must protect not only existing normative circles but the freedom to associate and *create and restructure* normative circles. Therefore I have argued that privacy should be seen as a social institution which maintains the boundaries of normative circles with the aim of preserving social freedom. The maintenance of many normative circles allows individuals to have social freedom and dignity and their entire lives are not controlled and scrutinised by any central power. Privacy is valuable to the extent that this freedom is valued.

I have tried to contribute to the debate on privacy by promoting a critical realist theory of privacy as an institution which serves the valuable end of associating with others and maintaining normative circles. There were hints of this understanding in the focus group discussions but largely understandings of privacy seemed to focus on the dichotomy between the individual and the central government with intimate relationships as the only mediator. All participants valued the individual but their views on the value and role of government differed. Some saw government as a threat while others saw it as the protector of privacy. In my view, this dichotomy is one central reason why the images of the future were problematic, some of them dystopian and others neglectful of current social and technological developments.

One focus group participant argued that the function of privacy is to recognise the human subject that shapes the state and society. My only addition to this would be that humans shape society *in interaction*. I would argue that discussions of privacy should be more sensitive to the ways in which society is constituted by the interaction of individuals within normative circles rather than seeing a dichotomy of the individual and the social system. In other words, discussions should consider the micro-macro continuum and the role of privacy in linking the different levels. Correspondingly, the divide between private and public should be seen within the context of various normative circles. There are thus various levels of publicity rather than only private and public. Information or persons are accessible to someone and private from others.

Viewing privacy as an institution means that it is a real social entity but it still relates to values. Current discussions about same-sex marriage demonstrate that institutions evoke feelings even though from a secular point of view they are social constructions. They evoke feelings because they are felt to have valuable ends. Once privacy is viewed as an institution with a particular function, threats to privacy can be set in context. Privacy is threatened by practices which violate norms concerning information flow and access and thus undermine the social freedom of individuals. The institution of privacy is protected better if its status as an institution is recognised rather than maintaining a simplistic notion of privacy as individual control of information and access or as an ultimate value which is nevertheless contradicted in everyday activities. As the focus group discussions demonstrated, in order to have real control rather than illusionary control, the preconditions for control, such as an awareness of the value of privacy and of threats, need to be in place.

From a theoretical point of view, this thesis aimed to take steps towards the integration of studying two kinds of futures: outcomes of existing processes and present ways of thinking about the future. Critical realism, in its ontological and epistemological versions, was seen to support the aims of critical futures studies in studying both aspects of the future. The conceptual discussion of privacy and the model of privacy dynamics explored the first aspect, which could be called objective futures or future presents, following Adam & Groves (2007). Here, the ontological critical realism promoted by Bhaskar (1979/2003), Patomäki (2006) and Elder-Vass (2010, 2012) was useful.

The empirical analysis of images of the future, in turn, explored subjective futures or present futures. Here, causal layered analysis, seen from the perspective of Bell's (1997) epistemological critical realism, was particularly helpful. The relationship between objective and subjective futures should be seen as dialectical. On the one hand, present futures influence future presents because images of the future influence the actions of individuals and groups in the present. On the other hand, knowledge of possibilities constrains images of the future, which makes images more achievable but it can also constrain them excessively. Therefore, a middle path between fatalism and utopia should be found in images of the future. This middle path would retain the agency of humans but abandon the illusions of omnipotence and of a completely open future.

Causal layered analysis proved to be a valuable analytical tool for examining the subjective futures of non-experts. The CLA process raised important questions regarding the problematic assumptions behind images of the future, such as the Cassandra myth, the lone ranger metaphor and the assumptions of slow, stable evolution and of a disciplined future. Considering these myth-level issues suggests new solutions at different levels. In addition, awareness of the underlying layers in images of the future makes it easier to have a dialogue between different images and to compare them with scientific knowledge on the past and present. Ultimately it enables both assessing and opening possibilities for future developments.

7 CONCLUSION

This study combined critical futures studies and critical realism in an investigation of images of the future of privacy. The theoretical ambition was to combine a tentative study of objective possibilities and processes affecting the future with a study of present understandings of the future, although the empirical material only permitted the study of the latter aspect. The thesis aimed to answer three main questions: how privacy and privacy dynamics can be conceptualised from a social perspective, how privacy is viewed by non-experts and what types of images of the future non-experts have.

In answer to the first question, I have argued that privacy protection is not only an issue of individuals' control over their own personal information or their right to be let alone. Instead, privacy was conceptualised as a social institution which maintains boundaries between normative circles in the context of normative intersectionality. Privacy as an institution protects individuals' possibilities to associate with others and to express and form their social identity together with others by participating in many social spheres. The function of privacy, then, is the protection of individuals' social freedom.

Changes in privacy occur when privacy norms are challenged by patterned practices where actors with particular interests use technologies to violate the privacy of individuals. Privacy protection is a social issue because these privacy violations have far-ranging impacts that influence power relations within society. Furthermore, these impacts may introduce new path dependencies which start a process of eroding privacy standards, as one of the images of the future anticipated.

In response to the second research question, four clusters of privacy conceptions were identified among focus group participants, and the participants were divided into four groups: privacy fundamentalists, privacy pragmatists, privacy individualists and privacy collectivists. These groups of participants had distinct views on the scope and importance of privacy, on privacy threats and solutions, on the responsibility for protecting privacy and on individuals' control over their privacy.

Corresponding to these four groups, four ideal-typical images of the future were crystallised. These were titled 'drift to low privacy', 'continuity and benign evolution', 'privatised privacy and an uncertain future' and 'a responsible future or moral decline'. The assumptions, worldviews and myths behind these images of the future were examined using the causal layered analysis method. Each image has its strengths and weaknesses. The individualistic images of the privacy fundamentalists and privacy individualists tended to be somewhat fatalistic, while the more collectivistic images tended to be somewhat utopian.

In a sense, the alternative images of the future are correctives of each other. An overemphasis on individual protection of privacy and the resulting uncontrolled future could be balanced by taking collective protection into account, and vice versa. However, there were also common problems with all the images. The dichotomies between individual and society, on the one hand, and between private and public, on the other hand, were viewed rather rigidly. It would be beneficial to have a more contextual view that takes into account various mediating structures between individual and society as well as the fact that privacy always means privacy *from* somebody and *for* something in a particular context. In addition, changes in privacy were viewed as stability, collapse or an entirely uncertain future. It would be beneficial to understand the ways in which privacy could change in a more nuanced way.

Therefore, a desirable future is not the hypothetical average of the ideal-typical images of the future. Instead, individuals should reflexively consider the different images of the future, the beliefs and myths behind them and the actions to which they lead. Even if individuals then decide to retain their old images of the future, they are more fully aware of the implications of their decision and of alternative conceptions. This reflection should be based on an attitude of responsibility towards the future and taking the consequences of one's actions into account.

This thesis has focused on images of the future within a limited set of focus group participants. The generalisability of the findings depends on whether similar images of the future of privacy exist in the larger population, within the Western context and beyond. This is an empirical question that merits further study, including cross-cultural comparisons. It is likely that the ideal-typical images of the future which were presented here would at least be refined by subsequent research.

There are also two other important areas for further study. Firstly, what are the sources of images of the future of privacy? Why do particular individuals and groups have particular images of the future? From this perspective, debates on privacy in the media and popular writings dealing with privacy could be analysed. Privacy is not only a discursively constructed phenomenon, but nevertheless it is important to consider the role of discourses in forming individuals' subjective views on privacy. Secondly, the link between images of the future and individuals' action could be studied more closely. In this thesis, the influence of images of the future on action was only assumed, but it would be beneficial to investigate how images of the future affect the choices that people make. For this, one would need to study the real behaviour of people, not only people's accounts of their behaviour.

Since privacy protection is a social issue, it relates to the question of desirable futures. The conceptual framework presented in this thesis enables envisioning desirable futures of privacy. What kind of society will we want to have in the future? What is the role of privacy in that society and how can it be achieved? I have argued that privacy, as the protection of the integrity of normative circles, contributes to a pluralist society where individuals have the opportunity to engage in many associations without being excessively controlled by a central power. If such a society is desired, privacy should be a part of it.

Creating bridges between present images of the future and real possibilities for the future is an ongoing challenge. On the one hand, images of the future need to take ongoing processes and current possibilities into account so that they can be credible enough to earn people's commitment. On the other hand, images of the future should inspire people towards creating the future and not merely submitting to social, economic and political necessities. In this dialectic, this thesis has argued for awareness of current images of the future as the first step. Once we are aware of our shared images of the future and the assumptions behind them, we can assess their truthfulness and their impacts on our behaviour, whether it is day-to-day behaviour or far-reaching choices made by decision-makers. However, changing our images of the future is only a first step. Thinking differently about the future must be followed by action.

What is the future of privacy as a social institution and how will the concept of privacy change in the future? Is it possible to protect privacy in the face of rapid technological progress, and if so, who should protect it? Who or what will threaten privacy in the future? This thesis has not attempted to provide a final word on these topics. The aim was rather to promote a dialogue of conceptions of privacy and of images of the future, but a dialogue which takes present threats and challenges into account. There is not one solution but many, just as there is not one future but many alternative futures. Through dialogue and collective action, we should transform dominating futures of privacy into masterable ones.

REFERENCES

Acquisti, A. (2009). Nudging privacy: the behavioral economics of personal information. *IEEE Security & Privacy Magazine*, *7*(6), 82–85.

Adam, B., & Groves, C. (2007). *Future Matters: Action, Knowledge, Ethics*. Leiden: Brill.

Ahlroth, J. (2010, March 9). Yksityisyydellä ei muka ole väliä? *Helsingin Sanomat*.

Alvesson, M., & Sköldberg, K. (2009). *Reflexive Methodology: New Vistas for Qualitative Research*. Los Angeles (Calif.): SAGE.

Arthur, C. (2013, June 3). Google Glass: is it a threat to our privacy? Retrieved March 8, 2013, from http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy

Auffermann, B., Luoto, L., Lonkila, A., & Vartio, E. (2012, February 13). PRACTIS Deliverable 4.2: Report on potential changes in privacy climates and their impacts on ethical approaches. Retrieved from http://www.practis.org/docs/PRACTIS,%20D4.2_Report%20on%20potential%20changes%20in%20privacy%20climates%20and%20their%20impacts%20on%20ethical%20approaches%20_Final%20version%2013.2.12_.pdf

Ayress, L. (2008). Thematic Coding and Analysis. In *The Sage encyclopedia of qualitative research methods* (pp. 868–869). Thousand Oaks, Calif.: Sage Publications. Retrieved from http://www.credoreference.com/book/sagequalrm

Baghai, K. (2012). Privacy as a human right: a sociological theory. *Sociology*, *46*(5), 951–965.

Bell, W. (1997). *Foundations of Futures Studies: Human Science for a New Era. Vol. 1, History, Purposes and Knowledge*. New Brunswick, N.J.: Transaction Publishers.

Bell, W. (2003). *Foundations of Futures Studies: Human Science for a New Era. Vol. 2, Values, Objectivity, and the Good Society*. New Brunswick, N.J: Transaction Publishers.

Bell, W., & Mau, J. A. (1971). Images of the future: theory and research strategies. In W. Bell & J. A. Mau (Eds.), *The Sociology of the Future; Theory, Cases, and Annotated Bibliography* (pp. 6–44). New York: Russell Sage Foundation.

Bell, W., Mau, J. A., Huber, B. J., & Boldt, M. (1971). A paradigm for the analysis of time perspectives and images of the future. In W. Bell & J. A. Mau (Eds.), *The Sociology of the Future; Theory, Cases, and Annotated Bibliography* (pp. 45–55). New York: Russell Sage Foundation.

Bellanova, R. (2011). Waiting for the barbarians or shaping new societies? A review of Helen Nissenbaum's Privacy In Context. *Information Polity*, *16*(4), 391–395.

Benn, S. I. (1971/1984). Privacy, freedom, and respect for persons. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 223–244). Cambridge: Cambridge University Press.

Bhaskar, R. (1979/2003). Transcendental realism and the problem of naturalism. In G. Delanty & P. Strydom (Eds.), *Philosophies of Social Science: The Classic and Contemporary Readings* (pp. 442–447). Maidenhead: Open University Press.

Bloustein, E. J. (1964/1984). Privacy as an aspect of human dignity: An answer to Dean Prosser. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 156–202). Cambridge: Cambridge University Press.

Boulding, K. E. (1962). The Image of the Future by Fred L. Polak. *Journal of Political Economy*, *70*(2), 192–193.

Boulding, K. E. (1956/1963). *The Image: Knowledge in Life and Society*. Ann Arbor: University of Michigan Press.

Brey, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. *NanoEthics*, *6*(1), 1–13.

Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, Mass.: Perseus Books.

Castells, M. (2000). *The Rise of the Network Society* (2nd ed.). Oxford: Blackwell.

Clegg, S. (2007). Ideal type. In G. Ritzer (Ed.), *Blackwell Encyclopedia of Sociology*. Blackwell Reference Online. Retrieved from http://www.blackwellreference.com/subscriber/tocnode.html?id=g9781405124331_chunk_g978140512433115_ss1-50

Dator, J. (1979). The futures of cultures or cultures of the future. In A. J. Marsella, R. G. Tharp, & T. J. Ciboroski (Eds.), *Perspectives on Cross-Cultural Psychology* (pp. 369–388). New York: Academic Press.

Dawes, S. (2011). Privacy and the public/private dichotomy. *Thesis Eleven*, *107*(1), 115–124.

De Jouvenel, B. (1967). *The Art of Conjecture*. New York: Basic Books.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.

Derrida, J. (1967/1997). *Of Grammatology*. (G. C. Spivak, Trans.). Baltimore: Johns Hopkins University Press.

Drucker, P. F. (1993). *Post-Capitalist Society*. New York: HarperBusiness.

Durkheim, E. (1895/1964). *The Rules of Sociological Method*. (S. A. Solovay & J. H. Mueller, Trans., G. E. G. Catlin, Ed.). New York: The Free Press.

Economist. (2012, March 3). The quantified self: Counting every moment. Retrieved May 20, 2012, from http://www.economist.com/node/21548493

Edge, D. (1995). The Social Shaping of Technology. In N. Heap, R. Thomas, G. Einon, R. Mason, & H. Mackay (Eds.), *Information Technology and Society: A Reader*. London: Sage.

Elder-Vass, D. (2010). *The Causal Power of Social Structures: Emergence, Structure and Agency*. Cambridge ; New York: Cambridge University Press.

Elder-Vass, D. (2012). *The Reality of Social Construction*. Cambridge: Cambridge University Press.

Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.

European Commission. (2012, January 25). EUROPA - PRESS RELEASES - Press Release - Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Retrieved May 13, 2013, from http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

European Union. (2000, December 7). Charter of Fundamental Rights of the European Union. Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, *7*(4), 185–200.

Foucault, M. (1969/2002). *Archaeology of Knowledge*. (A. M. Sheridan Smith, Trans.). London: Routledge.

Fried, C. (1968/1984). Privacy [A moral analysis]. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 203–222). Cambridge: Cambridge University Press.

Froomkin, A. M. (2000). The death of privacy? *Stanford Law Review*, *52*(5), 1461–1543.

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237.

Gavison, R. (1980/1984). Privacy and the limits of law. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 346–402). Cambridge: Cambridge University Press.

Hauptman, A., & Katz, O. (2011, July). PRACTIS Deliverable 2.2: Final Horizon Scanning Report. Retrieved from http://www.practis.org/docs/PRACTIS%20D2%202_130711final.pdf

Hedström, P., & Swedberg, R. (1998). Social mechanisms: An introductory essay. In P. Hedström & R. Swedberg (Eds.), *Social Mechanisms: An Analytical Approach to Social Theory*. Cambridge: Cambridge University Press.

Hedström, P., & Ylikoski, P. (2010). Causal mechanisms in the social sciences. *Annual Review of Sociology*, *36*(1), 49–67.

Heinonen, S. (2000). *Prometheus Revisited: Human Interaction with Nature Through Technology in Seneca*. Helsinki: The Finnish Society of Sciences and Letters.

Heinonen, S. (2001). Teknologian yhteiskunnallisesta merkityksestä eli tarina siitä heiluttaako "teknologiahäntä ihmiskoiraa" vai päinvastoin. *Futura*, *20*(2), 45–50.

Heinonen, S. (2011). Tekniikka ja ihminen - hybris vai harmonia uuden liiton askelkuviona? *Futura*, *30*(1), 95–98.

Henning, C. (2007). Institution. In G. Ritzer (Ed.), *Blackwell Encyclopedia of Sociology*. Blackwell Reference Online. Retrieved from http://www.blackwellreference.com/subscriber/tocnode.html?id=g9781405124331_chunk_g978140512433115_ss1-50

Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., & González Fuster, G. (2008). Legal safeguards for privacy and data protection in ambient intelligence. *Personal and Ubiquitous Computing*, *13*(6), 435–444.

Inayatullah, S. (1993). From "Who am I?" to "When am I?": Framing the shape and time of the future. *Futures*, *25*(3), 235–253.

Inayatullah, S. (1999). Reorienting futures studies. In Z. Sardar (Ed.), *Rescuing All Our Futures: The Future of Futures Studies* (pp. 49–60). Westport, CT.: Praeger.

Inayatullah, S. (2004a). Causal Layered Analysis: Theory, historical context, and case studies. In S. Inayatullah (Ed.), *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology* (pp. 1–52). Tamsui: Tamkang University Press.

Inayatullah, S. (2004b). Deconstructing and reconstructing the future: predictive, cultural and critical epistemologies. In S. Inayatullah (Ed.), *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology* (pp. 55–83). Tamsui: Tamkang University Press.

Inayatullah, S. (2004c). Appendix: The causal layered analysis pyramid. In S. Inayatullah (Ed.), *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology* (p. 543). Tamsui: Tamkang University Press.

Inayatullah, S. (2008). Six pillars: futures thinking for transforming. *Foresight*, *10*(1), 4–21.

Kant, I. (1785/2002). *Groundwork for the Metaphysics of Morals*. (A. W. Wood, Ed. & Trans.). New Haven: Yale University Press.

Karlsen, J. E., Øverland, E. F., & Karlsen, H. (2010). Sociological contributions to futures' theory building. *Foresight*, *12*(3), 59–72.

Kitzinger, J. (1995). Qualitative Research: Introducing focus groups. *BMJ*, *311*, 299–302.

Leeming, D. A. (2005a). Cassandra. In *The Oxford Companion to World Mythology*. Oxford: Oxford University Press. Retrieved from http://www.oxfordreference.com/view/10.1093/acref/9780195156690.001.0001/acref-9780195156690

Leeming, D. A. (2005b). Prometheus. In *The Oxford companion to world mythology*. Oxford: Oxford University Press. Retrieved from http://www.oxfordreference.com/view/10.1093/acref/9780195156690.001.0001/acref-9780195156690

Lobet-Maris, C., Grandjean, N., Colin, C., & Birnhack, M. (2012, December). PRACTIS Deliverable 5.2.

Lockton, V., & Rosenberg, R. S. (2005). RFID: The next serious threat to privacy. *Ethics and Information Technology*, *7*(4), 221–231.

Luhmann, N. (2002/2013). *Introduction to Systems Theory*. (P. Gilgen, Trans., D. Baecker, Ed.). Cambridge: Polity.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity.

Malmberg, L. (2012, June 22). Elämäni rekisterissä. *Helsingin Sanomat*.

Mannermaa, M. (2007). Living in the European ubiquitous society. *Journal of Futures Studies*, *11*(4), 105–120.

Mannermaa, M. (2008). *Jokuveli: elämä ja vaikuttaminen ubiikkiyhteiskunnassa*. Helsinki: WSOYpro.

Meadows, D. H. (2008). *Thinking in Systems: A Primer*. (D. Wright, Ed.). White River Junction, Vt.: Chelsea Green.

Murray, D., & Schwartz, J. (1997). Alarmism is an infectious disease. *Society*, *34*(4), 35–40.

Nissenbaum, H. F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books.

Patomäki, H. (2006). Realist ontology for futures studies. *Journal of Critical Realism*, *5*(1), 1–31.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

Polak, F. L. (1955/1973). *The Image of the Future*. (E. Boulding, Trans.). Amsterdam: Elsevier.

Popper, K. R. (1945/1966). *The Open Society and Its Enemies. Vol. 2, the High Tide of Prophecy: Hegel, Marx, and the Aftermath*. London :: Routledge & Kegan Paul.

PRACTIS Project Objectives. (2010). Retrieved May 15, 2013, from http://www.practis.org/index.asp?page=16

Rachels, J. (1975/1984). Why privacy is important. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 290–299). Cambridge: Cambridge University Press.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.

Reiman, J. H. (1976/1984). Privacy, intimacy and personhood. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 300–316). Cambridge: Cambridge University Press.

Rios, D. (2005). Social complexity and the micro-macro link. *Current Sociology*, *53*(5), 773–787.

Ritzer, G. (2001). Toward an integrated sociological paradigm: image of the subject matter. In *Explorations in Social Theory: From Metatheorizing to Rationalization* (pp. 79–99). London: SAGE.

Rubin, A. (2013). Hidden, inconsistent, and influential: Images of the future in changing times. *Futures*, *45*, S38–S44. doi:10.1016/j.futures.2012.11.011

Rubin, A., & Linturi, H. (2001). Transition in the making. The images of the future in education and decision-making. *Futures*, *33*(3-4), 267–305. doi:10.1016/S0016-3287(00)00071-9

Räikkä, J. (2007). *Yksityisyyden filosofia*. Helsinki: WSOY.

Schoeman, F. D. (1992). *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

Schwartz, P. (1996). *The Art of the Long View: Paths to Strategic Insight for Yourself and Your Company*. New York: Currency Doubleday.

Semantic Web - W3C. (2013). Retrieved May 20, 2013, from http://www.w3.org/standards/semanticweb/

Shefrin, B. M. (1986). Images of the future, futuristics and American politics. *Technological Forecasting and Social Change*, *30*(3), 207–219.

Slaughter, R. (2004). Beyond the Mundane: Reconciling Breadth and Depth in Futures Enquiry. In S. Inayatullah (Ed.), *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology* (pp. 147–161). Tamsui: Tamkang University Press.

Slaughter, R. (2008). What difference does “integral” make? *Futures*, *40*(2), 120–137.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.

Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press.

Swedberg, R. (2005). *Interest*. Maidenhead: Open University Press.

Tapio, P. (1999). Bellin tulevaisuusraamattu. *Futura*, *18*(1), 87–93.

Tapio, P., & Hietanen, O. (2002). Epistemology and public policy: using a new typology to analyse the paradigm shift in Finnish transport futures studies. *Futures*, *34*, 597–620.

Tavani, H. T. (2008). Informational privacy: concepts, theories, and controversies. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 131–164). Hoboken, N.J.: Wiley.

Van der Helm, R. (2009). The vision phenomenon: Towards a theoretical underpinning of visions of the future and the process of envisioning. *Futures*, *41*(2), 96–104.

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

Vasama, T. (2012, September 13). Brittikoulut asentavat valvontakameroita vessoihin. *Helsingin Sanomat*.

Weber, M. (1922/1978). *Economy and Society: An Outline of Interpretive Sociology, Vol. 1*. (G. Roth & C. Wittich, Eds.). Berkeley: University of California Press.

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum,.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.

Voros, J. (2008). Integral futures: an approach to futures inquiry. *Futures*, *40*(2), 190–201.

Wright, D. L. (2002). Applying Foucault to a future-oriented layered analysis in a post-bubble Japanese community. *Futures*, *34*(6), 523–534.

APPENDIX 1: THE FOCUS GROUP QUESTIONS

The following focus group questions were used in the focus group sessions conducted in April and May 2012 as part of Work Package 5 of the PRACTIS (Privacy – Appraising Challenges to Technologies and Ethics) project (Lobet-Maris et al., 2012).

Round 1 – Privacy as a commodity (30 minutes)

Imagine a Saturday's afternoon. You are entering in a large mall. At the entrance, a steward suggests you to wear the mall's electronic bracelet. This is the new big offer of the mall. This bracelet can record all your moves and transactions. The mall's Society is the operator of this system. The steward tells you that two major advantages are for you if you accept it. The first one is a 7 % discount on each transaction that you do. The second regards the personalization of the marketing that will be addressed to you, just fitting your recorded profile…

- What will you decide? Explain your motives and reasons.
- Could you consider personal data as something that belongs to the person, as a personal property that each of us can engage to get some advantages?

Round 2 – Privacy as a matter of concern (30 minutes)

- Do you consider that privacy matters and why do you think so?
- Is privacy a psychological issue related to the development of self or a political one related to the development of a democratic society?
- Do you think that the protection of privacy is an individual issue or a collective one?
- Do you think that privacy is in danger? And if yes, explain why?
- If you feel that privacy is in danger, what would you do to protect it?

Round 3 – The law considers that privacy protection is the protection of your personal data (30 minutes)

- For you, what do we have to protect when considering privacy protection?
- Do you consider your privacy as a question of personal data? Explain.
- Could you explain your vision of what privacy is – if necessary by using a term, a notion to characterize what you consider as private?

- When you say that you protect your privacy: what do you protect and against whom?

To protect you against misuse of your personal data, and hence to protect your privacy, the law obliges the data controllers/collectors to get your consent (specific informed indication) by which you signify your agreement to personal data relating to you being processed. It obliges them also to be transparent about the processing and, if you request it, to provide you with intelligible information regarding the performed processing of your data.

- Do you consider this consent as sufficient and efficient to protect your privacy?
- Do you consider this transparency and information obligation as sufficient and efficient to protect your privacy?

Round 4 – Recommendation for privacy (30 minutes)

- Do you think that privacy will still matter at horizon 2050? Or do you consider it as a misleading or as an outdated or obsolete concept?
- If you consider that privacy will still matter, what would you recommend to guarantee its protection?

APPENDIX 2: THEMES APPLIED TO THE EMPIRICAL MATERIAL

The following list presents the categories or themes under which the participants' views were grouped. The clustering of participants was based on the views that the participants expressed on these themes.

- Images of the future / Beliefs about the future
- Beliefs about the past
- Beliefs about the present
- Beliefs related to privacy: conceptions of privacy, functions of privacy etc.
- Privacy dynamics
    - Drivers of change / Threats
        - Actors
        - Interests
        - Technological systems
        - Practices
    - Solutions
        - Actors
        - Mechanisms
    - Individual
        - Action
        - Personal attitudes and values
        - Interests or benefits that compete with privacy