

# Framing the future of privacy: citizens' metaphors for privacy in the coming digital society

Matti Minkkinen<sup>1</sup>  · Burkhard Auffermann<sup>2</sup> · Sirkka Heinonen<sup>3</sup>

Received: 30 June 2017 / Accepted: 17 October 2017 / Published online: 24 October 2017  
© The Author(s) 2017. This article is an open access publication

**Abstract** Privacy is one of the pressing issues of the digital age. New technologies and surveillance practices continuously present new privacy threats. This paper reports an exploratory qualitative study on non-experts' metaphors for privacy in future society using focus group material from three countries: Finland, Germany and Israel. Using thematic analysis, four metaphorical frames for privacy are constructed: 'dodo', 'hemline', 'savings' and 'foundations of our home'. The frames are analysed using the causal layered analysis method to uncover their systemic and worldview components. Taken together, the metaphorical frames highlight two key concerns of individuals: their struggle for control over a dominating future, on the one hand, and the problem of trust in collective means of privacy protection, on the other hand. The article concludes that the views of non-experts need to be included in broad societal discussion about a desirable future society and the role of privacy in that society. This discussion needs to seriously consider systemic interconnections that challenge privacy as well as the whole ecosystem of metaphorical frames for privacy.

**Keywords** Metaphor · Privacy · Futures studies · Causal layered analysis

✉ Matti Minkkinen  
matti.minkkinen@utu.fi

<sup>1</sup> Finland Futures Research Centre, University of Turku, Rehtorinpellonkatu 3, 20500 Turku, Finland

<sup>2</sup> Finland Futures Research Centre, University of Turku, Åkerlundinkatu 2, 33100 Tampere, Finland

<sup>3</sup> Finland Futures Research Centre, University of Turku, Korkeavuorenkatu 25 A 2, 00130 Helsinki, Finland

## Introduction

Privacy is one of the pressing issues of the digital age. Privacy topics are discussed in the media every day, often in connection with new and emerging technologies. Current privacy threats include ubiquitous computing, radio-frequency identification, Big Data and behaviour in online social networks [1–5: 1]. Edward Snowden's revelations of NSA surveillance, in turn, have amplified the debate about the limits of governmental data collection [6]. While privacy may seem like a lost cause, there are also efforts to ensure privacy protection in the new technological landscape. Particularly in Europe, privacy issues are high on the agenda: the data protection reform process has culminated in the General Data Protection Regulation which was adopted on 27 April 2016.

Privacy has been studied extensively in recent decades [7, 8], and previous research projects have also studied possible futures of privacy in the context of emerging technologies [3, 9]. The stream of privacy literature has demonstrated that privacy fulfills the criteria of a wicked problem: it is multifaceted, there are many actors and possible solutions, and solutions are likely to create novel problems [10].

Privacy is also a deeply personal issue which influences the everyday life of ordinary citizens [11]. Therefore, the futures of privacy cannot be governed top-down and only discussed in specialist debates on data protection. We must consider the views of citizens in addition to experts and technology developers. In particular, citizens need to be empowered to consider preferred futures themselves. In foresight and anticipatory governance of emerging technologies, there is a growing trend towards citizen participation [12–14]. Even though participation brings new challenges, ordinary citizens need to take part in anticipatory discussions which touch on their everyday lives. By using a relatively long future time horizon, individuals can freely express their hopes and fears regarding privacy.

The views of non-experts can act as a reference when reforming privacy governance and designing information systems.

This article presents an explorative qualitative study on citizens' thinking on long-term futures of privacy. The intention is to map ordinary citizens' privacy conceptions and futures thinking rather than to uncover new knowledge about probable technological development or envision desirable futures. Causal layered analysis is used to study material from three focus groups conducted in 2012 in Finland, Germany and Israel. The future time horizon is 2050, although the exact year is not critical because anticipatory ideas are unlikely to be coded by year in individuals' thinking. In contrast to forecasting possible futures, the long-term future is used as a methodological tool to map citizens' thinking. In our searches, we have not been able to find literature that deals with citizens' anticipation of long-term privacy futures.

The article is structured as follows. In the first two sections, we will discuss the key concepts of the study, privacy conceptions and metaphorical futures thinking. Then, we will introduce the empirical data and the analysis methods. In the analysis section, we will present the results of the analysis followed by a discussion of the implications.

The qualitative analysis revealed four metaphorical frames for privacy in the future: privacy as the dodo, as the hemline, as savings and as foundations of our home. Privacy was conceptualised either in individualistic or collective terms. For the individualistic framing, the key concern is individual control. For the collective framing, in turn, the central question is trust in collective means of protecting privacy. The lessons from this study for societal debate are twofold. Firstly, broad societal debate is needed on a desirable society and the role of privacy in that society, taking into account systemic interconnections and possible system traps. Secondly, the discussion needs to consider the whole ecosystem of different privacy conceptions, worldviews and framing metaphors.

## Theoretical background

### Privacy conceptions

During several decades of privacy scholarship, defining privacy has proven to be difficult. Privacy is a complex phenomenon that is discussed in many fields including political science, computer science, legal theory and information systems [5: 67]. Privacy is also a controversial, normatively loaded and dynamically evolving concept [15: 11, 16: 132, 5: 67]. In contemporary research, privacy is generally defined as a multi-dimensional construct, encompassing physical space, social relations, psychological and decisional interference, and control over personal information [16: 135–144, 17: 12–13, 18].

The relational and contextual nature of privacy has also been emphasised in privacy scholarship. Privacy is a societal value [19: 220–231], and a contextual phenomenon that concerns different norms at home, in the workplace, in the online environment and in leisure activities [5, 15, 20]. Likewise, privacy violations are contextual, including surveillance, intrusion and illegitimate data aggregation [17: 40–49, 104]. Following Nissenbaum [5: 140], privacy can be defined briefly as sets of norms which govern acceptable data flows in different contexts.

However, for this paper, individual conceptions of privacy are more important than general definitions. Because individuals are the targets of privacy violations, discussions of privacy need to take into account how privacy is experienced by individuals [11: 47–48]. *Privacy conceptions* refer to the subjective ways in which individuals frame privacy: their perceived vulnerabilities and specific issues of concern. In particular, privacy conceptions refer to the cognitive aspects of privacy attitudes, as opposed to the affective aspects [18].

*Privacy concerns* are an established topic in the information systems literature, for instance in studies of privacy-related behaviour [21, 22]. However, privacy conceptions are more fundamental because the conception defines what an individual is concerned about [18]. Nevertheless, individual differences in privacy conceptions have thus far received little analytical attention [18].

In this article, we connect privacy conceptions to metaphorical frames of privacy in future society using focus group material. Miltgen and Peyrat-Guillard [23] have previously utilised focus groups in an extensive study of privacy concerns, but their focus was on understanding current privacy behaviour, disclosure and protection, rather than examining subjective privacy conceptions in the context of the long-term future.

### Cultural frames and metaphors for imagining futures

This article studies the cultural frames that ordinary citizens use when imagining futures of privacy. The long-term future is used as a tool to investigate these frames. Cultural frames are important because they shape expectations and discussions regarding the future [24]. Futures thinking is influenced by individuals' beliefs about the past, and about causes and effects as well as their broader cultural worldview [25, 26]. In futures research, the *image of the future*, an imagined future that influences action, is a closely related concept [25, 27, 28]. Recent psychological research has also examined futures thinking under the term *prospection*, which includes developing mental representations of a general or abstract state of the world ('semantic simulation') [29, 30]. In this article, the cultural frame is understood as the perspectivising lens that influences the perceived key issue or issues concerning futures of privacy.

Because cultural frames are complex, we have chosen to investigate them using metaphors. We understand metaphors in Lakoff and Johnson's sense, as conceptual mappings between different domains — something abstract understood in terms of something more concrete [31, 32]. In particular, we focus on understanding the role of privacy in future society through different metaphors. The assumption is that frames for imagining futures are largely metaphorical, but this claim is not studied in depth in this paper. Instead, we utilise metaphors as tools for communicating the essential aspects of a cultural frame.

Metaphors are a growing area of study within futures research [33]. To a large extent, the existing literature has focused on utilising metaphors for effective scenario building and successfully communicating scenarios [34, 35]. In contrast, in this paper we focus on metaphorical thinking of ordinary citizens outside explicit foresight processes. Existing images of the future influence individuals' behaviour and thus partly shape the emergent future [25: 32–33, 27: 1, 28: 82]. More importantly, it is necessary to become aware of existing frames as a first step towards discussing and shaping desirable futures.

Privacy conceptions, discussed in the previous chapter, constitute one part of the frames for understanding privacy futures. However, the broader frame also includes many other dimensions such as worldviews and ideologies. Causal layered analysis, introduced in the methodology section, is used as the framework for operationalising these concepts [36–38]. In the subsequent sections, we will first introduce the empirical data and then explain our approach to identifying and analysing metaphorical frames using thematic analysis and causal layered analysis.

## Empirical data and analysis methods

As empirical material, this article uses focus groups conducted in 2012.<sup>1</sup> Three focus group discussions were held: one in Finland, Germany and Israel.<sup>2</sup> Focus groups are a suitable data collection method for studying complex topics because they allow participants to explore issues using their own words [39]. Focus groups have been utilised to study privacy concerns in the context of new technologies [23, 40], but to our knowledge focus groups have not been used to study individuals' thinking on the future of privacy.

<sup>1</sup> The focus group sessions were held before the discussion initiated by Edward Snowden's disclosures, and thus they represent a snapshot of the debate at that time.

<sup>2</sup> In addition, focus group sessions were held in Belgium and Poland. However, the transcripts of these sessions did not allow distinctions between individual participants. Therefore they were unsuitable for our analysis focusing on individuals' metaphorical frames.

In total there were 28 participants in the three focus groups. The participants answered four rounds of open questions. The questions were prepared by one of the institutions in the PRACTIS consortium (see Appendix 1). The gender and age distributions of the participants are presented in Tables 1 and 2 below.

We analyse the frames using the causal layered analysis (CLA) method. Causal layered analysis is a qualitative futures research method that facilitates the in-depth study of beliefs about the future by dividing future-related texts into four layers: litany, system, worldview and metaphor [36–38]. In causal layered analysis, long-term futures are used as a methodological tool for examining present beliefs rather attempting to forecast possible futures. Analytical attention is drawn to futures thinking in the present, in this case the futures thinking of ordinary citizens.

Four layers of depth are identified in causal layered analysis. The litany level is the surface-level description of an issue or development. The system level explores assumptions regarding social, technological and other causes and systemic interrelations. The worldview level discusses the ideologies and paradigms which frame our understanding of issues. The final metaphor level includes the shared metaphorical interpretations which summarise the characteristics of the issue or development, and to which individuals are deeply committed [37: 11–15]. The layers of CLA are assumed to be connected to one another: metaphors and worldviews frame problems on the litany level [37: 3]. The layers are illustrated below in Fig. 1.

CLA is a versatile method and the layers can be interpreted in different ways. In this study, the goal is to investigate metaphorical frames for the future of privacy. Therefore the material needs to be divided according to core metaphors. We chose to divide the material according to clusters of participants, assuming that each individual has certain systemic beliefs, a certain worldview and core metaphor when considering futures of privacy, and that similar individuals can be grouped into clusters. We acknowledge that this is a simplification and individuals may simultaneously hold several conflicting views. Our interpretation of the layers is given below.

**Table 1** Gender distribution of the focus group participants

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

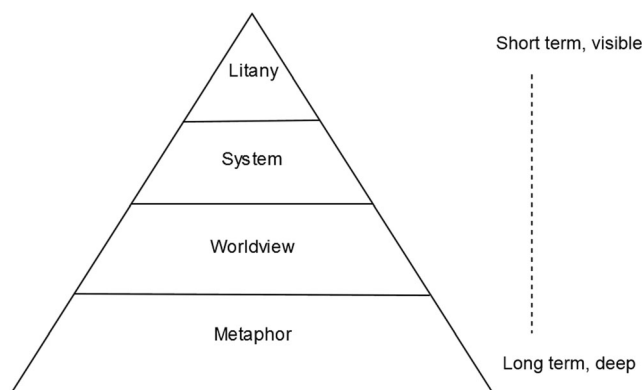
**Table 2** Age distribution of the focus group participants

Age (years)	Finland	Germany	Israel	Total
20–30	2	2	4	8
31–40	4	3	1	8
41–50	0	0	3	3
51–60	3	0	2	5
61+	1	1	2	4
Total	10	6	12	28

The *litany* layer is interpreted as the raw text data, ‘what the text says’. The *system* layer is divided into six sub-questions related to systemic concerns:

1. What is the participant’s *conception of privacy* and of the functions of privacy [18]? Is privacy viewed from a normative or descriptive perspective [5]? Is privacy primarily framed in terms of physical space, social relations, decisional interference or control [16–18]?
2. What are seen as *threats* or drivers of change? What are the roles of technology, state and corporate institutions and culture [42]?
3. *Which actors are seen as responsible* for protecting privacy (individuals, companies, the state) [23, 43]?
4. What kinds of *solutions* are presented?
5. Are individuals seen to have *control* over sharing personal information or is such control an illusion [44]?
6. How is the development of privacy over time perceived?

The *worldview* layer is understood through Mary Douglas’s cultural theory which identifies four ways of perceiving social relations (four ‘ways of life’): individualism, hierarchy, egalitarianism and fatalism [10, 45, 46]. In cultural theory, two dimensions are used for distinguishing between the different worldviews: the level of group pressure and the level of hierarchy. In

**Fig. 1** The causal layered analysis pyramid [41]

this study, the four worldviews are used in a heuristic manner without extensive analysis.

The fourth layer, *metaphor*, is interpreted through Lakoff and Johnson’s theory of metaphors as conceptual mappings between different fields [31, 32]. In this case, the abstract phenomenon of privacy is understood through some other phenomenon, which influences how the future role of privacy is envisioned. Thus metaphors take the form ‘privacy as something’. Moreover, we assume that metaphors are generally not directly mentioned in the discussions, and thus finding metaphors requires close reading and interpretation.

The six sub-questions on the system layer were used as the criteria for clustering the focus group participants.<sup>3</sup> First, the focus group discussions were coded in the Dedoose web application based on the themes listed above.<sup>4</sup> Then, each individual’s comments were investigated separately. We clustered the participants into four groups based on similar views on these themes. Quantitative clustering based on usage of words was deemed unreliable due to the complexity of privacy conceptions. Thus the clustering was done in a qualitative manner, relying on researchers’ judgments. This process is inevitably somewhat subjective since the questions listed above were not asked directly in the focus groups. Instead, views on these themes are derived from conversations which are complex social situations.

The clustering process began with identifying participants whose views clearly differed from each other and placing these participants in different clusters. Then participants that were similar to these initial ‘cluster centres’ were placed into the respective clusters. Ultimately, a relatively coherent clustering was achieved. In the next section, we present the four metaphorical frames that we identified.

## Four metaphorical frames for privacy in the coming digital society

In this section, each metaphorical frame is discussed and summarised in a table. The four frames are constructed as ideal types: hypothetical characterisations of a phenomenon in its purest form, aimed at capturing its essential features [47, 48: 18–22]. The composition of the clusters according to age, gender, and focus group is presented in Appendix 2.

### Privacy as the dodo

The first frame considers privacy as the dodo, that is, a species made extinct largely through human actions (Table 3). The

<sup>3</sup> The questions and differing views represent the ‘horizontal’ breadth of causal layered analysis [37].

<sup>4</sup> <http://www.dedoose.com>.

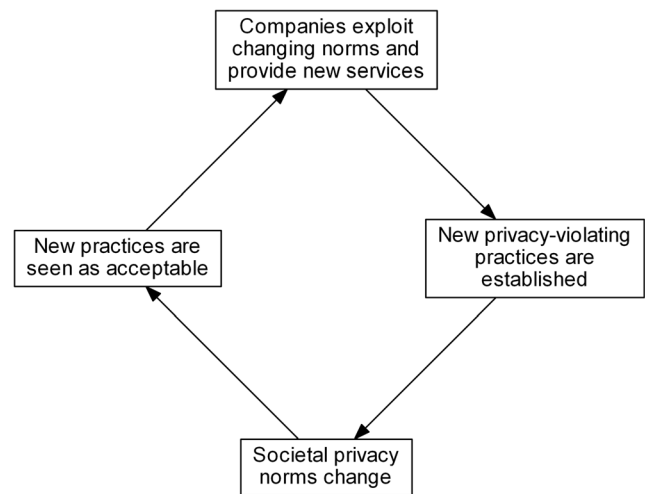
**Table 3** Causal layered analysis of privacy as the dodo (*n* = 12)

CLA layer	Analysis
Litany	Privacy is significantly diminished and surveillance and data collection using new technologies are everyday phenomena
System	<p>Conception of privacy: Normative. Privacy as the right to be let alone and wide control over personal information. Privacy is extremely important.</p> <p>Threats: Companies, governments and hedonistic individuals such as young people who unthinkingly share their data</p> <p>Responsible actor: Individual</p> <p>Solutions: Personal coping strategies</p> <p>Individual control: Control is illusory, individuals have lost control over their privacy</p> <p>Development: Gradual systemic drift to low privacy.</p>
Worldview	Fatalistic
Metaphor	Privacy as the dodo

dodo was a large flightless bird native to Mauritius which was made extinct in the 1600s when the Dutch hunted it and destroyed its habitat. Since then, the dodo has become a symbol of obsolescence. Extinction is preceded by a period when privacy as a value is critically endangered, which is how the current situation is seen in this frame. Privacy has then “gone the way of the dodo”, as the saying goes. More broadly, the fate of privacy also mirrors the process of environmental pollution and degradation [17: 177–178, 187, 5: 242–243]. Loss of privacy occurs much like climate change: economic interests, consumerist values and the systemic effects of contemporary lifestyle lead to irreparable damage to the environment and to privacy. Privacy is sacrificed to the contemporary technological lifestyle.

Companies and governments are seen as active agents and threats to privacy. Privacy protection is seen as the responsibility of individuals who are hedonistic consumers with little control over their privacy. In the Finnish focus group, one participant expressed the threat of shifting standards: “the threat is that we begin to consider control as self-evident and even compatible with our own interest” (male, 21–30 years). Another Finnish participant spoke of a numbing effect that continuous data collection has on people (female, 31–40 years). One Israeli participant claimed that “young people are willing to expose themselves completely and they don’t mind” (female, 61+ years).

In systems thinking, drift to low performance has been identified as one system trap. Drift to low performance means a situation where standards gradually fall because sub-average performance is assessed as the



**Fig. 2** Drift to low privacy

standard level and goals are set lower [49]. The mechanism of the drift to low privacy is illustrated in Fig. 2. The drift to low privacy is a systemic phenomenon, like the extinction of species.

Decreasing expectations of privacy lead to a decreasing overall level of privacy and vice versa. There is a negative feedback loop with no balancing loop to stop the drift [49]. Companies establish services and practices which diminish privacy norms, which in turn creates more demand for such services. The drift to low privacy is viewed as a path-dependent process where future options are dramatically reduced: “We can’t divert from the path we walk on this regard” (male, 51–60 years, Israel). Already today it is difficult for individuals to discard services such as Facebook and Google because they have become part of the normal lifestyle.

The *worldview* is fatalistic. Individuals tragically lose their autonomy to act against powerful actors and trends which determine the future. In Douglas’s cultural theory, the fatalistic worldview is the worldview of prisoners and servants, and more generally of culturally isolated and strictly supervised groups, which fits the image of lost privacy and autonomy [46].

**Privacy as the hemline**

In the second frame, privacy is both a shared value and a personal preference which is continuously negotiated and weighed against other interests including security, attractive services and effective healthcare. Privacy is thus the hemline: a fashion trend that emerges from the everyday choices of individuals, like clothing choices (Table 4). We choose our clothes based on our



**Table 4** Causal layered analysis of privacy as the hemline ( $n = 5$ )

CLA layer	Analysis
Litany	Privacy will remain important but it will be perceived differently
System	Conception of privacy: Privacy is a shared value and a personal preference. It is important but not the first priority. Threats: Criminals Responsibility: Shared between society and individuals Solutions: Common sense, traditional mechanisms, regulation Individual control: Real Development: Slow evolution through continuous negotiation
Worldview	Individualistic
Metaphor	Privacy as the hemline

preferences and our assessment of a particular situation, and generally our clothing choices do not have serious consequences. According to this frame, then, privacy is one value to be balanced in everyday situations.

On the *system* level, the future of privacy is characterised by continuity and relatively slow evolution compared to the present situation. Like fashion trends, privacy continuously evolves — in a certain period, the fashionable hemline is low and some years later it is higher before again returning to a low hemline. The perception of privacy will be different in the future due to new communications technologies, but privacy as an institution is not in great danger. Privacy will remain important and in the most fundamental aspects of life it will remain similar. Awareness of possible threats will lead to people holding on to privacy more tightly.

Traditional cultural and institutional methods of privacy protection such as consent and professional confidentiality and personal coping tactics are viewed as sufficient. Privacy is therefore in a state of relative equilibrium and there are no radical systemic challenges to current privacy norms. The main threats are seen to come from criminals engaging in identity theft, for example. In general, individuals are considered as active in controlling their privacy. The evolution of privacy occurs through pragmatic and contextual negotiation, weighing the benefits and risks. As one participant put it, “we shouldn’t get hysterical” (male, 51–60 years, Finland). 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).

The *worldview* is individualistic. Although privacy is viewed as a shared value, individuals are continuously engaging in negotiation with their privacy. If the benefits are attractive, privacy can be flexibly negotiated. When negotiating privacy, we need to pragmatically consider the threats related to revealing aspects of ourselves in each context.

### Privacy as savings

In the third frame, privacy is seen as savings, that is, assets that some can afford to have while others must use most of their personal information as currency (Table 5). According to this frame, personal information is a commodity and it is the property of an individual, which means that individuals are free to trade with it. Privacy, then, is a type of restriction on the free flow of personal information. The argument is that there will be significant changes in lifestyle by 2050, and technological progress is the central driving force behind these changes. Privacy will exist in highly individualised and unequal forms. Those who have skills and money have a high level of privacy, while others have little privacy. Technological progress changes lifestyles, and privacy will have to be adapted to the new technological surroundings. Legislation will always lag years behind technological developments. Because of the rapidity of the change, the future is uncertain and it is difficult to know much about the changes that are to come.

**Table 5** Causal layered analysis of privacy as savings ( $n = 4$ )

CLA layer	Analysis
Litany	There is a free market of personal information with individualised and unequal privacy
System	Conception of privacy: Individualised. Personal information is a commodity that can be traded, and privacy is a regulating factor in this trading. Threats: New technologies, government Responsible actor: Individual Solutions: Individual’s abilities, purchasing power and common sense Individual control: Possible but unequally divided Development: Unstoppable evolution of technology and marketisation
Worldview	Individualistic
Metaphor	Privacy as savings

From the *system* perspective, privacy is seen as highly individualised. It is the responsibility of individuals as consumers to protect their own privacy. The free market of personal information is seen as the natural state, and privacy regulation introduces restrictions and market distortion. In the privacy literature, some commentators have argued that giving individuals a property interest in their personal information would lead to individuals having more control over their information, since they can bargain with it and exchange it for other goods in the market [16: 134]. However, others criticise this development because it privatises the social phenomenon of privacy and neglects the public and collective value of privacy [50]. In addition, if individuals must cope alone, there is little protection for those who are incapable of protecting their own privacy.

The *worldview* is individualistic. In principle, each individual has equal opportunities to protect their privacy and to trade with it. However, because individuals are concerned with private benefit, concentration of wealth and power mean that egalitarian ideals are not reached [46]. In general, privacy is intimately connected to individual freedom. From the individualistic perspective, privacy means the freedom to pursue happiness in one’s own way as long as no harm is done to others. A liberal individualist discourse is prominent within privacy theorising, and it has been argued that historically privacy emerged together with individualism [15: 113–114]. The view of privacy as protection of freedom is especially prominent in the United States [51].

**Privacy as foundations of our home**

The fourth metaphorical frame presents privacy as foundations of our home, a crucial element for maintaining our personal identity and our democratic society (Table 6). Privacy is

**Table 6** Causal layered analysis of privacy as foundations of our home (*n* = 7)

CLA layer	Analysis
Litany	We have a moral obligation to protect privacy by legislation
System	Conception of privacy: Control over information and access, and also a shared value. Privacy is a sacred value which cannot be traded. Threats: Lack of awareness, knowledge and transparency Responsible actor: Society Solutions: Broad regulatory framework Individual control: Real Development: Equilibrium: privacy maintains democracy and democracy maintains privacy.
Worldview	Egalitarian
Metaphor	Privacy as foundations of our home

a sacred value which is inviolable and must be protected. Sacred values may not be traded off against secular ones such as money [52]. Therefore the flow of personal data needs to be strictly regulated and citizens need to be protected against inequality and discrimination. This is in contrast to the ‘hemline’ and ‘savings’ frames, where privacy may be negotiated and traded. The sacred value framing presents a ‘challenge and response’ development narrative [53: 144–147] where the community continually faces challenges relating to privacy protection, but these challenges are tackled by the democratic political process. Ensuring privacy protection requires continuous collective efforts. There is a parallel to current discussions on climate change and the necessary transition to sustainable energy. Maintaining a desirable level of privacy in the future may require societal transitions similar to those in energy policy. Ultimately the attitude regarding the future is optimistic: the future can be controlled, like in Jim Dator’s archetypal ‘disciplined society’ image [54].

On the *system* level, this participant cluster emphasises the social importance of privacy and the moral obligation to protect privacy. The future depends on the model that current generations set for future generations, and therefore we must act responsibly. One participant (male, 31–40 years, Germany) argued that privacy is a cultural value that is connected to the Enlightenment, and also a political value as “part of the protection of citizens which is one of the main tasks of society and the state”. This is seen as important for maintaining democracy.

This framing presents a virtuous cycle which maintains privacy. Privacy as a shared value enables the maintenance of the democratic public, which then protects privacy by regulating exposure and trade of information. This in turn maintains privacy as a shared value. 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 discourse, the freedom of humans is not challenged by the government, because the individual and society are not seen as conflicting forces but rather society has an active role in shaping individuals [55].

The *worldview* is egalitarian. An Israeli participant (female, 21–30 years) stated that privacy means protection from inequality. They continued: “Privacy must be uniform: everybody must be exposed or concealed in the same amount”. Without privacy, everybody would have a different ‘colour’ and could be treated differently. Because privacy is a collective value, the downgrading of privacy by some will cause loss of privacy for all. This expresses the ideal of a strongly bonded group with few ranking or grading rules between its members [46].

## Discussion

### An ecosystem of frames as different types of futures

The four metaphorical frames can be interpreted as different kinds of thinking about the future. Futures thinking is always *modal*, which means that it relates to necessity, possibility and contingency [56, 57]. The modality of futures thinking means that imagined futures are linked to human agency in different ways, and they may serve different functions, such as describing likely events, calling for action or presenting future opportunities. A useful frame for categorising futures thinking is de Jouvenel's [58: 55] division of forecasts into primary, secondary and tertiary (historical) forecasts. Table 7 below illustrates the frames based on these frameworks.<sup>5</sup>

Using de Jouvenel's [58] typology, 'dodo' is a primary forecast: this is the undesirable 'business-as-usual' future, which becomes real if nothing is done. It should be read as a cautionary tale that is intended as a prompt for action to protect privacy. The 'foundations of our home' frame is similar to a secondary forecast: it indicates that we must collectively uphold privacy as a value. The 'hemline' and 'savings' frames, in turn, can be understood as historical forecasts, trying to imagine what could happen in the complex interplay of different actors. From this perspective, imagining slow evolution or uncertainty are understandable reactions to considering the future.

Moreover, the underlying conceptions of privacy are different in the different frames. This is crucial because the conceptions of privacy determine the focus for imagining the future of privacy. In other words, they answer the question "The future of what?" and indicate how important this question is considered to be. Due to differing privacy conceptions, then, the central question about the future of privacy is different. For the individualistic privacy conception, the question is about optimism or pessimism regarding individual control. For the collective privacy conception, the central question is maintaining privacy as a shared value through collective means. Table 8 below illustrates the privacy conceptions and key issues.

We argue that these frames in fact constitute an *ecosystem* of frames rather than mutually incompatible alternatives. Douglas [46] states that all worldviews (individualism, fatalism, hierarchy, egalitarianism) are needed, and governance solutions that impose one organising principle will fail. Rather than constituting alternatives, all of these frames are needed, and the diversity of cultural frames is a key factor in shaping

<sup>5</sup> There are also many other frameworks for categorising futures thinking such as Tapio and Hietanen's typology [59], but this one was chosen for its simplicity and because it can be used to categorise general futures thinking as opposed to professional futures research.

**Table 7** The metaphorical frames likened to different types of forecasts

Metaphorical frame	Type of forecast [58]
Privacy as the dodo	Primary
Privacy as the hemline	Historical
Privacy as savings	Historical
Privacy as foundations of our home	Secondary

a resilient future. If the frames are seen as an ecosystem, the crucial question is whether the ecosystem is diverse enough and whether these frames adequately represent different worldviews.

Whether the frames are adequate for representing the different worldviews needs more empirical research, but some preliminary remarks can be made. The 'savings' frame presents both the benefits and drawbacks of individualism. Arguably it is more plausible than the 'hemline' frame which presumes continuity in an era of rapid change. The 'dodo' frame, in turn, begs the question why some individuals are able to see grave threats to privacy while others are blissfully ignorant. Finally, the 'foundations of our home' frame is an attractive description of a desirable future, but the shared value basis that it presumes may be problematic in a multicultural society. From this ecosystem perspective, it is undesirable to search for one ultimate metaphor of privacy. Instead, it is desirable to diversify futures thinking and to consider emergent novelty rather than repeating conventional discourses [60].

### Implications for policy, research and public discussion

Considering policy implications, some limitations need to be taken into account. Firstly, the intention of these metaphorical frames is not to contribute directly to policy-making by providing desirable visions. Instead, they raise important themes in the privacy debate. Secondly, the current study is exploratory with a limited set of participants. Thirdly, the focus group design (see Appendix 1) focused on current threats and the section on futures was relatively short. Finally, most of the discussion was negatively framed, lacking discussions of privacy-enhancing technologies (PETs) or beneficial market mechanisms.<sup>6</sup>

The metaphorical frames highlight two key themes in the privacy debate: individual control and trust in collective privacy protection.<sup>7</sup> The first theme is the

<sup>6</sup> Arguably this negative framing is inherent in the modern concept of privacy which focuses on conditions of its violation, not its realisation [42].

<sup>7</sup> Similar themes were found by Miltgen and Peyrat-Guillard [23], who identified control, regulation, trust and responsibility as foci of privacy concerns in a focus group study



**Table 8** Privacy conception and the key issue of the future of privacy

	Privacy as mundane	Privacy as highly important
Privacy as an issue of individual control	Optimism about control (savings)	Pessimism about control (dodo)
Privacy as an issue of collective governance	Manageable change (hemline)	Challenge and response (foundations of our home)

*individual's struggle for control and agency* in a future consisting largely of dominating elements. There is a clear danger to individuals' autonomy if they are given only illusory control regarding their personal information. The 'dodo' and 'savings' frames express similar privacy threats but the agency of individuals is viewed differently. The former frame emphasises lack of control while the latter suggests that control is possible but unequally distributed.

For most of the focus group participants, the future of privacy is something that emerges beyond their control. This tendency was clearest for those expressing the 'dodo' frame. This feeling of helplessness is problematic for privacy policy-making, particularly in Europe. One of the stated aims of the EU data protection reform is to empower citizens [61]. At the time of writing, it is too early to tell whether the process is successful, but Blume [62] argues that the General Data Protection Regulation does not empower citizens and this is actually not its goal. The theme of control actually includes two issues: whether citizens feel that they have control over their personal data, and whether they feel they can influence the debate on privacy protection. If there are widespread feelings of powerlessness, corrective measures such as increasing awareness are urgently needed.

The second theme is *trust in collective privacy protection mechanisms* such as privacy legislation. There is an ongoing debate whether binding privacy legislation or market-based solutions are preferable for 'future-proofing' privacy protection. The 'dodo' and 'savings' frames express skepticism about the effectiveness of privacy legislation, while the 'hemline' and 'foundations of our home' frames express more optimism and trust. If complex privacy legislation is drafted without public understanding or trust, the risk is that citizens become alienated from the privacy debate. It is important that in a democratic society citizens understand the reasoning behind privacy protection rules and that they are able to use the means of privacy protection available to them. This is particularly important as the participatory governance has been a central aim within the European Union in recent years [63].

Both nation states and EU institutions need to work on establishing trust in privacy legislation, because if privacy protection is left to individuals, privacy is likely

to become unequally distributed. This is already the case with technological tools such as public key encryption and virtual private networks which are difficult to utilise for most citizens. Similarly, technical debates about data protection principles are unlikely to make citizens feel empowered and trustful. Establishing trust in EU institutions is particularly challenging in the current atmosphere of uncertainty regarding the future of the EU.

The question about privacy should be put into broader societal context. The key question is what kind of future society we want to live in and what role privacy has in this society, given current trends towards digitalisation and increasing surveillance. Privacy conceptions and metaphorical frames form an ecosystem where diversity is important rather than categorising conceptions as correct or mistaken. Therefore policy-making on privacy should not be made in a technocratic manner without public engagement. This means that the discussion should not be dominated by one frame such as liberal individualism, administrative efficiency or the fight against terrorism. Instead, transparent and inclusive debate is the prerequisite for seeking desirable futures of privacy. The debate should include the whole spectrum of worldviews and the whole cast of privacy-related actors including citizens, policy-makers, technology developers and companies [43].

The final implication of these metaphorical frames is that a broad systemic view is needed in privacy research and public discussion. We need to move beyond enumerating individual privacy threats and identify and analyse potential system traps such as the drift to low privacy. These traps can be analysed in similar ways as social-ecological system traps [64]. The interests which drive privacy actors' choices need to be part of the discussion because these are crucial in systemically producing privacy threats. Knowledge is also needed on cross-sectoral interrelations, that is, how privacy is influenced by decision-making in other fields such as security and traffic policy. Climate researchers discuss the water-energy-food nexus, highlighting the close linkages between these areas [65]. This raises the question what kind of 'nexus' is formed by privacy and other policy fields. In addition, the systemic concepts of system traps and nexus raise the question of systemic transition.

Where is the privacy system currently heading and do we need path creation or ‘mindful deviation’ to reach a more desirable future [66]?

There are some indications at present of this broad discussion about desirable futures and the role of privacy. The EU data protection reform is seeking to tackle trust issues by establishing credible and effective general privacy rules. The recent documentary *Democracy* tracks the reform, suggesting that central players within the EU institutions were active in promoting data protection in Europe [67]. However, the General Data Protection Regulation has also been described as a “monster text” because of the difficulty of interpreting its layered meanings [62].

The MyData concept, in turn, aims to give control to consumers while also ensuring that organisations can make use of data collection [68, 69]. Similarly, the Privacy by Design concept harnesses engineering and product design to protect privacy [70]. Privacy impact assessments aim to track the systemic privacy impacts of decisions [71]. These developments suggest that it is possible to retain a sense of agency on the road to the unknown future.

## Conclusion

This article investigated metaphorical frames for the future of privacy using focus group data and causal layered analysis. The aim was to map citizens’ thinking on futures of privacy using metaphorical frames. Thematic analysis was used to cluster focus group participants into four groups with distinct views on the conception of privacy, on privacy threats and solutions, on the responsibility for protecting privacy and on control over privacy.

Four metaphorical frames for privacy futures were constructed: ‘dodo’, ‘hemline’, ‘savings’ and ‘foundations of our home’. The systemic drivers and worldviews behind these frames were examined using causal layered analysis. The privacy conceptions expressed in the frames differed along two key axes: individualistic or collective framing of privacy and privacy viewed as a highly important or relatively mundane issue. The analysis highlighted two key themes: individuals’ struggle for control over a dominating future and trust in the effectiveness of privacy legislation. Rather than alternative futures, the frames can be interpreted as different types of projections: primary (what will happen if nothing is done), secondary (what should be done) and historical (what could happen). Therefore they relate to human agency in different ways.

The study was exploratory but nonetheless the results have significant research and policy implications. Further studies could elaborate on the metaphorical frames that were constructed in this study, and perhaps modify or refute them. One interesting area for subsequent research is cultural differences. Would the frames be radically different if a similar study was conducted in China or in Nigeria? In which cultures is the question of the future of privacy even relevant, and should it be relevant? Another area of study is the influence of media on these frames. Does recent media coverage or social media discussion of privacy issues significantly impact the expressed views of non-experts, or are their views relatively stable?

Privacy protection is one of the key concerns in the ongoing digital transformation. The debate about privacy needs to be part of a broad and inclusive debate about the desirable future direction for society. The whole ecosystem of metaphorical frames and cast of privacy actors, including citizens, need to be part of the debate. In addition, potential system traps and systemic interconnections need to be studied further. In order to avoid traps and to find a path towards a desirable future, policy-makers, companies and researchers need to take individuals’ conceptions of privacy and its future seriously.

**Acknowledgements** The focus group study was conducted in the PRACTIS (Privacy – Appraising Challenges to Technologies and Ethics) project which was 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. 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. See <http://www.practis.org/>.

**Publisher’s note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## Appendix 1: focus group questions

### Round 1 – Privacy as a commodity (30 min)

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 min)

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 min)

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 min)

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: composition of clusters

The following tables present the composition of the participant clusters according to gender, focus group and age. Note that the group of participants is not a representative sample but a small group selected to include diverse participants. Therefore the numbers are only indicative. Percentage shares are not used because they are easily misleading for such small numbers.

**Table 9** Clusters according to gender

Cluster	Number of women	Number of men	Total
Privacy as the dodo	4	8	12
Privacy as the hemline	2	3	5
Privacy as savings	1	3	4
Privacy as foundations of our home	4	3	7
Total	11	17	28

**Table 10** Clusters according to focus group

Cluster	Finland	Germany	Israel	Total
Privacy as the dodo	3	2	7	12
Privacy as the hemline	4	0	1	5
Privacy as savings	2	1	1	4
Privacy as foundations of our home	1	3	3	7
Total	10	6	12	28

**Table 11** Clusters according to age

Cluster	20–30	31–40	41–50	51–60	61+	Total
Privacy as the dodo	2	3	2	2	3	12
Privacy as the hemline	2	0	0	3	0	5
Privacy as savings	1	2	1	0	0	4
Privacy as foundations of our home	3	3	0	0	1	7
Total	8	8	3	5	4	28

**Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

## References

- Brey PAE (2012) Anticipatory ethics for emerging technologies. *NanoEthics* 6:1–13. <https://doi.org/10.1007/s11569-012-0141-7>
- Hauptman A, Katz O (2011) PRACTIS deliverable 2.2: final horizon scanning report
- De Hert P, Gutwirth S, Moscibroda A et al (2009) Legal safeguards for privacy and data protection in ambient intelligence. *Pers Ubiquit Comput* 13:435–444. <https://doi.org/10.1007/s00779-008-0211-6>
- Lockton V, Rosenberg RS (2005) RFID: the next serious threat to privacy. *Ethics Inf Technol* 7:221–231. <https://doi.org/10.1007/s10676-006-0014-2>
- Nissenbaum HF (2010) *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books, Stanford
- MacAskill E, Guardian US Interactive Team (2013) NSA files decoded: Edward Snowden's surveillance revelations explained. *The Guardian*
- Minkinen M (2015) Futures of privacy protection: a framework for creating scenarios of institutional change. *Futures* 73:48–60. <https://doi.org/10.1016/j.futures.2015.07.006>
- Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. *MIS Q* 35:980–A27
- Auffermann B, Luoto L, Lonkila A, Vartio E (2012) PRACTIS deliverable 4.2: report on potential changes in privacy climates and their impacts on ethical approaches
- Ney S, Verweij M (2015) Messy institutions for wicked problems: how to generate clumsy solutions? *Environ Plann C: Gov Policy* 33:1679–1696. <https://doi.org/10.1177/0263774x15614450>
- Lobet-Maris C, Grandjean N, Colin C, Birnhack M (2012) PRACTIS deliverable 5.2
- van der Helm R (2007) Ten insolvable dilemmas of participation and why foresight has to deal with them. *Foresight* 9:3–17. <https://doi.org/10.1108/14636680710754138>
- Cairns G, Šliwa M, Wright G (2010) Problematizing international business futures through a critical scenario method. *Futures* 42: 971–979. <https://doi.org/10.1016/j.futures.2010.08.016>
- Krabbenborg L (2016) Creating inquiry between technology developers and civil society actors: learning from experiences around nanotechnology. *Sci Eng Ethics* 22:907–922. <https://doi.org/10.1007/s11948-015-9660-2>
- Schoeman FD (1992) *Privacy and social freedom*. Cambridge University Press, Cambridge
- Tavani HT (2008) Informational privacy: concepts, theories, and controversies. In: Himma KE, Tavani HT (eds) *The handbook of information and computer ethics*. Wiley, Hoboken, pp 131–164
- Solove DJ (2008) *Understanding privacy*. Harvard University Press, Cambridge
- Steijn WMP, Vedder A (2015) Privacy under construction. *Sci Technol Hum Values* 40:615–637. <https://doi.org/10.1177/0162243915571167>
- Regan PM (1995) *Legislating privacy: technology, social values, and public policy*. University of North Carolina Press, Chapel Hill
- Baghai K (2012) Privacy as a human right: a sociological theory. *Sociology* 46:951–965. <https://doi.org/10.1177/0038038512450804>
- Schwaig KS, Segars AH, Grover V, Fiedler KD (2013) A model of consumers' perceptions of the invasion of information privacy. *Inf Manag* 50:1–12. <https://doi.org/10.1016/j.im.2012.11.002>
- Kokolakis S (2017) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Comput Secur* 64:122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Miltgen CL, Peyrat-Guillard D (2014) Cultural and generational influences on privacy concerns: a qualitative study in seven european countries. *Eur J Inf Syst* 23:103–125. <https://doi.org/10.1057/ejis.2013.17>
- Beckert J (2013) Imagined futures: fictional expectations in the economy. *Theory Soc* 42:219–240. <https://doi.org/10.1007/s11186-013-9191-2>
- Bell W, Mau JA (1971) Images of the future: theory and research strategies. In: Bell W, Mau JA (eds) *The sociology of the future: theory, cases, and annotated bibliography*. Russell Sage Foundation, New York, pp 6–44
- Rubin A (2013) Hidden, inconsistent, and influential: images of the future in changing times. *Futures* 45:S38–S44. <https://doi.org/10.1016/j.futures.2012.11.011>
- Polak FL (1973) *The image of the future*. Elsevier, Amsterdam
- Bell W (1997) *Foundations of futures studies: human science for a new era, vol 1, history, purposes and knowledge*. Transaction Publishers, New Brunswick
- Baumeister RF, Vohs KD (2016) Introduction to the special issue: the science of prospection. *Rev Gen Psychol* 20:1–2. <https://doi.org/10.1037/gpr0000072>
- Szpunar KK, Spreng RN, Schacter DL (2016) Toward a taxonomy of future thinking. In: *Seeing the future: theoretical perspectives on future-oriented mental time travel*. Oxford University Press, Oxford, pp 21–35
- Lakoff G, Johnson M (1980) *Metaphors we live by*. The University of Chicago Press, Chicago
- Lakoff G (1996) *The contemporary theory of metaphor. Metaphor and thought*
- Inayatullah S, Izgarjan A, Kuusi O, Minkinen M (2016) Metaphors in futures research. *Futures*. <https://doi.org/10.1016/j.futures.2016.04.004>
- Bowman G, MacKay RB, Masrani S, McKiernan P (2013) *Storytelling and the scenario process: understanding success and*



- failure. *Technol Forecast Soc Chang* 80:735–748. <https://doi.org/10.1016/j.techfore.2012.04.009>
35. Carbonell J, Sánchez-Esguevillas A, Carro B (2017) From data analysis to storytelling in scenario building. A semiotic approach to purpose-dependent writing of stories. *Futures* 88:15–29. <https://doi.org/10.1016/j.futures.2017.03.002>
  36. Inayatullah S (1998) Causal layered analysis: poststructuralism as method. *Futures* 30:815–829
  37. Inayatullah S (2004) Causal layered analysis: theory, historical context, and case studies. In: Inayatullah S (ed) *The causal layered analysis (CLA) reader: theory and case studies of an integrative and transformative methodology*. Tamkang University Press, Tamsui, pp 1–52
  38. Inayatullah S (2015) The continued evolution of the use of CLA: using practice to transform. In: Inayatullah S, Milojević I (eds) *CLA 2.0: transformative research in theory and practice*. Tamkang University Press, Tamsui, pp 13–21
  39. Kitzinger J (1995) Qualitative research: introducing focus groups. *BMJ* 311:299–302
  40. Morton A (2013) All my mates have got it, so it must be okay: constructing a richer understanding of privacy concerns—an exploratory focus group study. In: *Reloading data protection*. Springer Nature, pp 259–298
  41. Inayatullah S (2004) Appendix: the causal layered analysis pyramid. In: Inayatullah S (ed) *The causal layered analysis (CLA) reader: theory and case studies of an integrative and transformative methodology*. Tamkang University Press, Tamsui, p 543
  42. John NA, Peters B (2016) Why privacy keeps dying: the trouble with talk about the end of privacy. *Inf Commun Soc* 20:284–298. <https://doi.org/10.1080/1369118x.2016.1167229>
  43. Raab C, Koops B-J (2009) Privacy actors, performances and the future of privacy protection. In: Gutwirth S, Pouillet Y, Hert P et al (eds) *Reinventing data protection?* Springer, Dordrecht, pp 207–221
  44. Westin AF (1967) *Privacy and freedom*. Atheneum, New York
  45. Boschetti F, Price J, Walker I (2016) Myths of the future and scenario archetypes. *Technol Forecast Soc Chang* 111:76–85. <https://doi.org/10.1016/j.techfore.2016.06.009>
  46. Douglas M (2006) A history of grid and group cultural theory. Semiotics Institute Online, Toronto <http://semioticon.com/sio/courses/the-group-grid-model/>
  47. Clegg S (2007) Ideal type. *The blackwell encyclopedia of sociology*. <https://doi.org/10.1111/b.9781405124331.2007.x>
  48. Weber M (1978) *Economy and society: an outline of interpretive sociology*, vol vol. 1. University of California Press, Berkeley
  49. Meadows DH (2008) *Thinking in systems: a primer*. Chelsea Green, White River Junction
  50. Cohen JE (2000) *Examined lives: informational privacy and the subject as object*. Social Science Research Network, Rochester
  51. Whitman JQ (2004) The two western cultures of privacy: dignity versus liberty. *Yale Law J* 113:1151–1221. <https://doi.org/10.2307/4135723>
  52. Tetlock PE (2003) Thinking the unthinkable: sacred values and taboo cognitions. *Trends Cogn Sci* 7:320–324. [https://doi.org/10.1016/s1364-6613\(03\)00135-9](https://doi.org/10.1016/s1364-6613(03)00135-9)
  53. Schwartz P (1996) *The art of the long view: paths to strategic insight for yourself and your company*. Currency Doubleday, New York
  54. Dator J (1979) The futures of cultures or cultures of the future. In: Marsella AJ, Tharp RG, Ciboroski TJ (eds) *Perspectives on cross-cultural psychology*. Academic, New York, pp 369–388
  55. Farrelly C (2004) Communitarianism. In: *Introduction to contemporary political theory*. SAGE Publications Ltd, London, pp 97–118
  56. Booth C, Rowlinson M, Clark P et al (2009) Scenarios and counterfactuals as modal narratives. *Futures* 41:87–95. <https://doi.org/10.1016/j.futures.2008.07.037>
  57. Miller R (2007) Futures literacy: a hybrid strategic scenario method. *Futures* 39:341–362. <https://doi.org/10.1016/j.futures.2006.12.001>
  58. Jouvenel B de (1967) *The art of conjecture*. Basic Books, New York
  59. 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. [https://doi.org/10.1016/S0016-3287\(02\)00003-4](https://doi.org/10.1016/S0016-3287(02)00003-4)
  60. Miller R, Poli R, Rossel P (2014) The discipline of anticipation: exploring key issues. UNESCO, The Rockefeller Foundation, Paris
  61. European Commission (2012) COMMUNICATION from the commission to the european parliament, the council. In: *The european economic and social committee and the committee of the regions safeguarding privacy in a connected world a European data protection framework for the 21st century COM/2012/09 final*
  62. Blume P (2014) The myths pertaining to the proposed general data protection regulation. *Int Data Privacy Law* 4:269–273. <https://doi.org/10.1093/idpl/ipu017>
  63. Marxsen C (2015) Open stakeholder consultations at the European level – voice of the citizens? *European Law Journal* 21:257–280. <https://doi.org/10.1111/eulj.12084>
  64. Boonstra WJ, de BFW (2013) The historical dynamics of social-ecological traps. *Ambio* 43:260–274. <https://doi.org/10.1007/s13280-013-0419-1>
  65. Leck H, Conway D, Bradshaw M, Rees J (2015) Tracing the water-energy-food nexus: description, theory and practice. *Geography Compass* 9:445–460. <https://doi.org/10.1111/gec3.12222>
  66. Boon WP, Aarden E, Broerse JE (2015) Path creation by public agencies — the case of desirable futures of genomics. *Technol Forecast Soc Chang* 99:67–76. <https://doi.org/10.1016/j.techfore.2015.06.038>
  67. Bernet D (2015) *Democracy: im rausch der daten*
  68. Iemma R (2016) Towards personal data services: a view on some enabling factors. *Int J Electron Gov* 8:58. <https://doi.org/10.1504/ijeg.2016.076690>
  69. Kuikkaniemi K, Poikola A, Pitkänen O (2014) My data fueling wellbeing applications. In: *Proceedings of the 2014 workshops on advances in computer entertainment conference - ace '14 workshops*
  70. Hustinx P (2010) Privacy by design: delivering the promises. *Identity in the Information Society* 3:253–255. <https://doi.org/10.1007/s12394-010-0061-z>
  71. Clarke R (2009) Privacy impact assessment: its origins and development. *Comput Law Secur Rev* 25:123–135. <https://doi.org/10.1016/j.clsr.2009.02.002>