

Accepted Manuscript

Title: Futures of Privacy Protection: A Framework for
Creating Scenarios of Institutional Change

Author: Matti Minkkinen

PII: S0016-3287(15)00090-7

DOI: <http://dx.doi.org/doi:10.1016/j.futures.2015.07.006>

Reference: JFTR 2041



To appear in:

Received date: 2-4-2015

Revised date: 24-6-2015

Accepted date: 16-7-2015

Please cite this article as: Matti Minkkinen, Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change, *Futures* (2015), <http://dx.doi.org/10.1016/j.futures.2015.07.006>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change

Matti Minkkinen^{a,*}

^a*Finland Futures Research Centre, Turku School of Economics, FI-20014 University of Turku*

Abstract

The future of privacy is a topical issue in the context of debates on mass surveillance and the increasing prevalence of social media sites in everyday life. Previous scenario studies on privacy have focused on macro trends and on forecasting technological developments, and claims about causal influences have remained implicit. This article presents an alternative approach for constructing scenarios of privacy protection. The article focuses on privacy protection as a social institution and builds on the theory of gradual institutional change. The article presents a scenario framework which includes three stages: 1) outlining the dynamics of privacy protection, 2) tracing historical processes and constructing a causal narrative, and 3) creating event-based scenarios. The resulting scenarios are narratives of plausible chains of events which are based on the results of the previous stages. The key difference to typical scenario approaches is the focus on specific actors and types of event sequences in privacy protection. The argument is that by lowering the level of abstraction in this way, researchers and decision-makers can gain a more profound understanding of possible future challenges in privacy protection and of key leverage points in the institutional change process.

Keywords: privacy, privacy protection, data protection, scenario, institution, institutional change

1. Introduction

We live in a surveillance society and privacy is an illusion. This is the message that is increasingly being delivered by media and academic discussions, with only a hint of exaggeration (e.g. Von Drehle, 2013). The future of privacy is a much debated issue in the context of Edward Snowden's revelations of mass surveillance and the prevalence of social media sites in everyday life. There is an increasing recognition that privacy as a cultural value may be under threat, especially due to the rise of new surveillance technologies and the post-9/11 emphasis on national security. The recent terrorist attacks against the Charlie Hebdo magazine in Paris have sparked new concerns over increasing state surveillance (Toor, 2015). Some commentators are ready to deem privacy an antiquated value that has no place in contemporary society, while privacy advocates continue to emphasise the importance of privacy for a democratic society.

Given the rapid spread of information technologies in recent decades and their profound impacts on societal conditions, the future of privacy is clearly an issue that warrants detailed investigation.

*Corresponding author

- A framework for creating privacy protection scenarios is presented.
- Privacy protection is defined as a social institution.
- The focus is on actor dynamics, historical processes and event-based scenarios.
- The framework allows identifying leverage points in institutional change processes.

Accepted Manuscript

Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change

Abstract

The future of privacy is a topical issue in the context of debates on mass surveillance and the increasing prevalence of social media sites in everyday life. Previous scenario studies on privacy have focused on macro trends and on forecasting technological developments, and claims about causal influences have remained implicit. This article presents an alternative approach for constructing scenarios of privacy protection. The article focuses on privacy protection as a social institution and builds on the theory of gradual institutional change. The article presents a scenario framework which includes three stages: 1) outlining the dynamics of privacy protection, 2) tracing historical processes and constructing a causal narrative, and 3) creating event-based scenarios. The resulting scenarios are narratives of plausible chains of events which are based on the results of the previous stages. The key difference to typical scenario approaches is the focus on specific actors and types of event sequences in privacy protection. The argument is that by lowering the level of abstraction in this way, researchers and decision-makers can gain a more profound understanding of possible future challenges in privacy protection and of key leverage points in the institutional change process.

Keywords: privacy, privacy protection, data protection, scenario, institution, institutional change

1. Introduction

We live in a surveillance society and privacy is an illusion. This is the message that is increasingly being delivered by media and academic discussions, with only a hint of exaggeration (e.g. Von Drehle, 2013). The future of privacy is a much debated issue in the context of Edward Snowden's revelations of mass surveillance and the prevalence of social media sites in everyday life. There is an increasing recognition that privacy as a cultural value may be under threat, especially due to the rise of new surveillance technologies and the post-9/11 emphasis on national security. The recent terrorist attacks against the Charlie Hebdo magazine in Paris have sparked new concerns over increasing state surveillance (Toor, 2015). Some commentators are ready to deem privacy an antiquated value that has no place in contemporary society, while privacy advocates continue to emphasise the importance of privacy for a democratic society.

Given the rapid spread of information technologies in recent decades and their profound impacts on societal conditions, the future of privacy is clearly an issue that warrants detailed investigation. While the future of privacy has been actively discussed in the media, futures of privacy have less frequently been studied using the tools of futures research. When privacy scenarios have been constructed, they have focused either on forecasting future technologies and their possible impacts or on broad-brush generalisations about societal dynamics (e.g. 6, 1998; Auffermann, Luoto, Lonkila, & Vartio, 2012; De Hert, Gutwirth, Moscibroda, Wright, & González Fuster, 2009). These studies have served an important role as overviews of possible developments to

1
2 guide decision-making. However, because of the high level of abstraction, specific causal claims
3 about development paths have remained somewhat implicit.
4

5 This article contributes to addressing this research gap. The aim of the article is to propose a
6 framework for constructing scenarios of the future of privacy protection. The article proceeds in
7 three parts. First, existing literature on the futures of privacy is outlined to identify research
8 gaps. The next step is to define the conceptual focus for investigating privacy and the futures
9 of privacy. The article focuses specifically on privacy *protection* as an institution which is
10 continuously developed through the interaction of societal actors. I will argue that institutional
11 change, and particularly the theory of gradual institutional change presented by Mahoney &
12 Thelen (2009), is an appropriate conceptual framework for studying futures of privacy protection.
13 Finally, I will present a framework for creating scenarios of privacy protection. The framework
14 includes three stages: 1) outlining the dynamics of privacy protection to gain analytical focus, 2)
15 tracing historical processes and constructing causal narratives, and 3) creating scenarios based on
16 identified mechanisms and potential chains of events. By lowering the level of abstraction from
17 macro trends to actors and event sequences, the framework enables making plausible conjectures
18 about future paths and identifying leverage points.
19
20
21

22 **2. Studies on futures of privacy**

23

24 In this section, I will present a brief overview of existing studies on futures of privacy before
25 presenting my own approach. There is no single agreed definition of privacy in the theoretical
26 literature. Privacy has been discussed in disciplines ranging from philosophy and legal theory
27 to information systems and computer science (Nissenbaum, 2010, p. 67). In the 1990s, Perri 6
28 (1998, p. x) listed 22 scholarly fields where privacy has been discussed and stated that claiming
29 to have done a comprehensive literature review “would be ridiculous”. Since then, the literature
30 has grown considerably. Privacy is often considered as an umbrella term, a cluster concept or
31 a loose network of constructs, and thus it is difficult to relate privacy studies to one another
32 (DeCew, 1997, p. 61; Smith, Dinev, & Xu, 2011). Privacy is also an evolving concept which
33 perhaps cannot be conclusively defined (Tavani, 2008a, p. 132). Nevertheless, it is important to
34 have a conceptual focus, particularly in future-oriented studies.
35

36 Many books and articles on privacy include a brief speculation on the future of privacy, often
37 in the final chapters (e.g. Moore, 1984; Nissenbaum, 2010; Solove, 2008; Westin, 2003). In
38 this section, I will only discuss those accounts which employ scenario methods or other futures
39 methodology. In addition, future-oriented studies with only a passing mention of privacy have
40 been omitted. Nevertheless, the selection of studies is bound to remain selective, since the
41 literature is overwhelmingly large: at the time of writing, a search on the ScienceDirect system
42 provided more than 13,000 results for the search terms “(privacy OR ‘data protection’) AND
43 future AND scenario”.
44

45 In previous studies, scenarios of the future of privacy have been primarily constructed on the basis
46 of ongoing trends and macro-level driving forces. The focus tends to be on emerging technologies
47 and their projected impacts. Brin (1998) and Mannermaa (2008) argue that transparency and
48 surveillance will increase in the future and this might lead to desirable or undesirable scenarios
49 depending on macro-level societal dynamics such as which actors or sector gains predominance.
50 Mannermaa’s approach is rooted in an evolutionary scheme of big waves of technological and
51 societal changes. In this context, privacy is likely to diminish in the transition to the ubiquitous
52 information society. Brin, in turn, identifies four surveillance scenarios on a high level of
53
54
55
56
57
58
59
60
61
62
63
64
65

1
2 abstraction. Brin's work, however, is more polemical than scholarly, arguing strongly in favour of
3 more transparency.
4

5 Perri 6 (1998) has conducted a comprehensive study on the futures of privacy, with the aim of
6 formulating better, culturally viable public policies around privacy. His argument is that the
7 future of privacy depends on how macro-level conflicts of values are resolved, and legislation
8 only has a secondary role. The strength of Perri 6's work is that he argues against technological
9 and other kinds of determinism, and he highlights value conflicts as a driving force of social
10 change (6, 1998, pp. 12–14). He also places privacy disputes into the wider frame of informational
11 capitalism. In terms of futures methodology, Perri 6 outlines drivers of change and constructs a
12 certainty-importance grid and cross-impact analysis. He constructs three privacy scenarios by
13 using a method based on a cultural theory and the interplay of four conceptions of private life:
14 civic republicanism, liberalism, egalitarianism and fatalism (6, 1998, ch. 15). The background
15 data is based on a literature review, expert interviews and a survey conducted in the United
16 Kingdom (6, 1998, p. 83). The study is ambitious and insightful but the focus remains on
17 macro-level dynamics with little attention paid to the events and mechanisms through which
18 privacy as an institution changes.
19

20 EU projects have also been conducted on futures of privacy. The SWAMI¹ project identified
21 four dark privacy scenarios related to ambient intelligence (Ahonen et al., 2010; De Hert et al.,
22 2009). The methods consisted of expert workshops and internal brainstorming, and the resulting
23 scenarios are highly useful as warnings about potential developments in ambient intelligence.
24 The PRACTIS² project, in turn, created five privacy scenarios using expert interviews and
25 future-oriented brainstorming sessions (Auffermann et al., 2012). The focus in PRACTIS was on
26 directions of broad drivers in five domains: society, legislation, economics, politics and values. By
27 using this holistic approach, the PRACTIS project made a significant contribution, particularly
28 to understanding the changing conceptions of privacy and 'privacy climates', as well as the policy
29 implications of these changes.³
30

31 C. J. Bennett & Raab (2006 pp. xxvi-xxvii) briefly mention four possible visions of future privacy
32 protection from the policy perspective. The advantage of their approach is that two of the
33 visions (race to the bottom and trading-up) are based on specified socioeconomic mechanisms,
34 and there is a clear conceptual framework of privacy regimes. However, the future scenarios are
35 only mentioned and not developed in detail.⁴
36

37 In summary, previous research has significantly increased our knowledge of potential privacy
38 threats and of the changing nature of privacy, and research projects have also outlined possible
39 solutions to privacy threats. As grounds for decision-making, the studies have been commendable.
40 However, from the social science perspective employed in this article, previous studies have
41 suffered from four shortcomings. Firstly, the scenarios have tended to be constructed through
42 heuristic exercises using expert workshops or interviews. The scenario technique has been either
43 individual judgment or some variant of morphological analysis, focusing on structural descriptions
44 of the future rather than events and development paths (Bishop, Hines, & Collins, 2007). As a
45 result, development over time has not been investigated in detail.
46
47

48 ¹Safeguards in a World of Ambient Intelligence

49 ²Privacy – Appraising Challenges to Technologies and Ethics

50 ³The author was involved in the PRACTIS project during spring 2012.

51 ⁴Pew Research Center has also recently conducted a research project on the futures of privacy on the Internet.
52 The study was an exercise in expert prediction without significant use of futures methodology (Pew Research
53 Center, 2014).
54
55

Secondly, the level of abstraction has been rather high. Researchers have investigated futures of privacy on a high level of abstraction and aggregation, focusing on macro-level drivers in broad categories. The focus on macro-level drivers and outcomes is problematic because contemporary social science highlights the necessity of studying the microfoundations of macro-level outcomes (Hedström & Ylikoski, 2010). Due to the focus on macro-level drivers, claims about causal influences and possible development paths have remained implicit.

Thirdly, the studies have not been embedded in a theoretical understanding of privacy and of the mechanisms through which privacy changes. In other words, there has not been a clear analytical focus and conceptual framework for investigating privacy. Finally, studies have not employed empirical evidence from the history of privacy protection in support of conjectures about the future.

The combined effect of these shortcomings is that research on futures of privacy has not focused in detail on the actors and sequences of events that may influence changes in privacy protection. In the following sections, I will suggest an alternative approach to constructing privacy scenarios which builds on the perspective of institutional change and the parallel between futures research and historical social science.

3. Studying futures of privacy: an institutional perspective

3.1. Privacy protection as a social institution

The intention in this article is to develop a perspective on privacy which enables empirically studying futures of privacy. For this purpose, it is useful to consider different levels of analysis in more depth. Ritzer (2001, p. 93) identifies two axes of social analysis: micro–macro and subjective–objective. Social analysis can be positioned along these axes: some approaches highlight subjective aspects such as norms and values while others aim to explain society from a more behavioural, realist perspective. Similarly, research approaches may focus on interaction between individuals at the micro level, on group dynamics or on macro-societal phenomena. In table 1, I have heuristically placed definitions of privacy into this framework.⁵

Table 1: Definitions of privacy

	Subjective definitions: experiences, norms, values	Objective definitions: mechanisms, functions
Micro: individuals	Privacy as control over personal information (Westin, 1967).	Privacy as precondition for dignity, respect and moral autonomy (Benn, 1971; Bloustein, 1964; Reiman, 1976). Privacy as the right to be let alone: protection from intrusion, interference and information access (Gavison, 1980; Tavani, 2008b; Warren & Brandeis, 1890).

⁵Smith et al. (2011) and Bélanger & Crossler (2011) have divided privacy research into four analytical levels: individual, group, organisation and society. Fuchs (2011), in turn, presents a division of privacy theories into subjective and objective theories. To my knowledge, these axes have not been combined before.

	Subjective definitions: experiences, norms, values	Objective definitions: mechanisms, functions
Relational: relationships and social groups	Privacy as norms which ensure appropriate flows of information (Nissenbaum, 2010).	Privacy as necessary for intimate relationships through differential sharing of personal information (Fried, 1968; Rachels, 1975). Privacy as a dynamic process of negotiating boundaries and forming self-identity in social relations (Cohen, 2012; Petronio, 2002; Schoeman, 1992; Steeves, 2009).
Macro: society	Privacy as a shared value (Regan, 1995).	Privacy as a feature of social structure and a socially created need (Baghai, 2012; Moore, 1984; Solove, 2008; Westin, 2003).

The table shows that privacy has been defined in various ways: as control, as norms, as a value, as a mechanism for maintaining relationships and as a feature of social structure. Mapping analytical levels in this way demonstrates that privacy has been defined in various ways partly because theorists have focused on different explanatory levels and thus on different aspects of privacy. In particular, the liberal individualist tradition has been strong and the emphasis has been on the importance of privacy for the individual: the need for psychological well-being, creativity and so on (Fuchs, 2011; Regan, 1995). Theorists have only relatively recently begun to discuss the societal importance of privacy, that is, the benefits that *all* members of society gain when privacy is protected in a society. The focus on the individual is true also in empirical research. In two comprehensive reviews of privacy research, the authors found that there were considerably more studies focused on the individual level than the group, organisational or societal level (Bélanger & Crossler, 2011; Smith et al., 2011). Bélanger & Crossler (2011) explicitly state that more studies of privacy should be conducted at the societal level of analysis.

The focus on the individual level of analysis is particularly problematic for futures research, because a holistic system-level view is one of the defining features of futures research (Bell, 1997). Therefore, in this article I will focus on the macro level: on cultural and societal aspects of privacy. Because of the recurring definitional confusion, information systems researchers have concentrated on privacy *concerns* as the central construct (Smith et al., 2011, p. 988). However, I will suggest an alternative focus for futures researchers. In my view, it is fruitful to focus on the phenomenon of privacy *protection* as a society-level goal and activity.⁶ The reason is that from a futures and social science perspective, it is more appropriate to consider the preconditions and safeguards for achieving a desired level of privacy than attempting to predict future privacy concerns.

The definition of privacy protection in this article is the following: *Privacy protection is a social institution, a group of norms, that governs practices involving flows of information and access to individuals.* A brief definition of an institution is “the fixing of stereotyped social interactions in the form of rules” (Henning, 2007). In this sense, institutions are social regimes which involve rule-making and also interpretation and implementation of rules (Streeck & Thelen,

⁶The closely related term ‘data protection’ is used particularly in Europe. The term ‘privacy protection’ is used here in a more comprehensive sense, encompassing both data flows and access to individuals.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

2005). Institutions are commonly viewed as relatively enduring features of social life that are slow and difficult to change (Mahoney & Thelen, 2009). Privacy has been previously defined as a right, an interest, a condition and so on (Nissenbaum, 2010), but to my knowledge, privacy protection has not been explicitly defined as an institution.⁷ Solove (2008, p. 74) lays the foundations for this definition by stating that privacy is not a “resource existing in the state of nature that the law must act to conserve”, but rather “something we construct through norms and the law”.

The focus on norms is beneficial because it is an intermediary position between considering particular interests and broad societal values. Several authors have considered privacy as a set of norms or rules (Nissenbaum, 2010; Solove, 2008). Nissenbaum (2010) argues that privacy norms concern flows of information in a particular context such as healthcare or education, but there may also be privacy norms that are common across contexts. Privacy norms are either codified in legislation at the national or supranational level or protected solely by trust and informal sanctions. Means of privacy protection can be seen as a continuum ranging from informal cultural cues to formal binding legislation with several intermediary means such as industry self-regulation and privacy standards (C. J. Bennett & Raab, 2006).

3.2. Futures research and the perspective of institutional change

In the previous section, privacy protection was defined as an institution. Next, this definition will be put into temporal perspective, and then the key question is how privacy protection changes over time and how future scenarios can be constructed. There is a rich tradition of scenario thinking with diverse approaches and techniques such as intuitive logics, morphological analysis, the Manoa School method, *la prospective* and the six pillars approach to futures thinking (Bishop et al., 2007; Bradfield, Wright, Burt, Cairns, & Van Der Heijden, 2005; Inayatullah, 2008). What, then, is the added value of presenting yet another scenario approach rather than selecting a suitable one? My argument is that existing scenario approaches have not focused on analytically explaining institutional change processes where human action has a central role. Especially in intuitive logics approaches, scenario building is considered as an art related to strategic planning and organisational learning which helps decision-makers to explore uncertainties and perceive new strategic opportunities (e.g. Schwartz, 1996).

The aim in this article is to present an approach for analytically studying plausible futures of privacy protection by constructing issue-based scenarios. In this context, it is useful to understand the future as latent possibilities inherent in complex social systems (Bell, 1997, pp. 76–80; Poli, 2011; Wilkinson, Kupers, & Mangalagiu, 2013). A scenario, then, tells the story of the actualisation of some of these inherent possibilities based on actions that are taken. Knowledge about objective possibilities may never be certain and assumptions about the functioning of systems in the future are problematic, but I hope to demonstrate that this understanding of the future gives a foundation for considering short to medium-term futures on the basis of historical and theoretical knowledge.

The approaches of alternative futures and critical futures studies present possible frameworks which recognise the complexity of societal change (Dator, 2009; Inayatullah, 2004). The strength of these approaches is that they can reveal assumptions behind future-related statements and help to consider genuinely different futures. However, in critical futures studies, the focus has been

⁷This definition has been hinted at by previous theorists, at least Haggerty & Ericson (2000), Schoeman (1992) and Solove (2008). In addition, C. J. Bennett & Raab (2006) use the concept of privacy *regimes* which is similar to formal institutions.

1
2 shifted from explaining social change to knowledge and epistemology—ideologies and cultural
3 myths that explain and influence change—and visioning alternative futures (Inayatullah, 2002).
4 Due to this analytical focus, it is difficult to investigate processes of institutional change from a
5 purely critical futures studies perspective, especially if the focus is on formal institutional aspects
6 such as legislation and treaties.
7

8 Formal systems modelling is one way of discovering developments that unfold over time, but here
9 it is infeasible because privacy protection is difficult to operationalise and measure (C. J. Bennett
10 & Raab, 2006, pp. 235–266). How can the futures of privacy then be studied? In the following,
11 I will present a perspective which draws on theories of institutional change before presenting a
12 scenario framework in the next section.
13

14 The conceptual focus on privacy protection as an institution is useful because it highlights
15 the historically relative nature of privacy. Rather than a timeless right or value, privacy is a
16 historically changing phenomenon. This definition directs future-oriented research to focus on
17 studying processes of institutional change. Because an institution is essentially a set of rules,
18 the study of institutional change means explaining the processes and mechanisms through which
19 these rules change.
20

21 Institutional changes are often slow processes involving complex causality, and therefore a
22 historical point of view is necessary in studying them (Barkey, 2009). The importance of
23 a historical perspective holds also for futures researchers. At a minimum level, a historical
24 perspective means studying phenomena in historical time and balancing historical specificity with
25 theoretical generalisation (Thelen, 1999). The parallel between historical studies and futures
26 research is fairly uncontroversial. For Ossip Flechtheim (quoted in Masini, 2010), futurology is
27 intimately linked with historically oriented sociology, and more recently, authors have argued for
28 a connection between historical research and futures research (e.g. Kaivo-oja, Katko, & Seppälä,
29 2004; Staley, 2007).
30

31 However, I would argue that futures researchers should go a step further and integrate insights
32 from contemporary historical social science into futures research. Historically oriented social
33 science explains change processes by referring to causal *mechanisms*. As Höjer & Mattsson
34 (2000) point out, instead of making predictions based on perceived trends and patterns, futures
35 researchers need to understand the mechanisms that produce empirically observable trends. A
36 mechanism can be briefly defined as the “cogs and wheels” of the causal process that brings
37 an outcome that is explained. A mechanism-based explanation discloses how specific entities,
38 activities and relations produce an outcome (Hedström & Ylikoski, 2010). Mechanisms are closely
39 related to processes: a process is what mechanisms can trigger (Manzo, 2007).
40

41 In the study of institutional change, it is important to differentiate between the mechanisms
42 of institutional genesis, reproduction and change. Different mechanisms may be operating in
43 the reproduction and change of an institution than those which were originally responsible for
44 its genesis (Mahoney, 2000a, p. 512). For the purposes of this paper, it is more important to
45 understand reproduction and change in privacy protection than its original genesis.
46

47 In future-oriented studies on privacy, the detailed study of change mechanisms has usually not
48 been a central focus. Previous research on the futures of privacy has focused on macro-level drivers
49 and outcomes, whether technological or cultural. This approach is problematic because social
50 scientists and philosophers of science have challenged explanations that are based on relations
51 between macro variables. Instead of macro-level relationships, mechanism explanations are rooted
52 in actors' behaviour on the micro level using approaches such as rational choice, network analysis,
53 agent-based modelling and institutional analysis (Barkey, 2009; Hedström & Ylikoski, 2010).
54
55

1
2
3 Macro-level outcomes, such as a decrease in the level of privacy protection, are not caused by
4 any macro driver or a set of megatrends, but instead they emerge from the complex interplay of
5 actors with various motives, similar to the 'invisible hand' of the market mechanism.

6
7 Within the historical social science framework, the future is the relatively open outcome of ongoing
8 historical processes. According to historical sociologists, societal processes are path-dependent
9 but not deterministic (Barkey, 2009). History plays a role in defining possibilities, but it does not
10 determine the choices of actors nor the outcomes. Thus large-scale societal processes do not follow
11 any predetermined path, such as digitalisation or the rise of transparency. Instead, the societal
12 outcomes are produced by the interaction of many actors. The point is not that institutions
13 cannot be rationally designed, but that such design has to consider social mechanisms and the
14 interplay of societal actors.

15
16 Therefore, in contrast to the focus on macro drivers (intuitive logics approaches) or ideologies
17 (critical futures studies), I will suggest an explicit focus on the actors, causal mechanisms and
18 chains of events that effect changes in the level of privacy protection. If we recall Ritzer's (2001)
19 framework, the aim is to explain how macro phenomena are produced by interactions at the
20 micro level.

21
22 In addition to highlighting causal complexity, it is important to understand that institutional
23 change is not a natural process which can be explained through unchanging laws of nature.
24 Instead, it is a societal process where human actions have transformative power. Therefore
25 the decisions of actors and their reactions to other actors need to be considered.⁸ Arguably a
26 *narrative* mode of explanation, focusing on sequences of action, is more suitable for understanding
27 institutional changes than the variable-centred explanations that are standard in futures research
28 (Abell, 2004). Variables have an important role as concise descriptions of past and future states,
29 but variables do not cause historical changes, action does.

30
31 The final central concept in addition to processes, mechanisms and actors is the concept of
32 historical *events*. In institutional change, human actions constitute events which change some
33 aspect of the social world (Abell, 2004). Other actors then react to the events and the changed
34 circumstances, and thus a chain or sequence of events is formed (Mahoney, 2000a). Because
35 human actions are crucial at each stage of such sequences, outcomes such as future states of
36 privacy protection cannot be posited without analysing the prior sequence of events. Therefore it
37 is more fruitful to consider scenarios as event sequences rather than structural descriptions of the
38 future (Bishop et al., 2007).

39
40 Historical institutionalism and evolutionary futures studies provide a set of conceptual tools for
41 understanding change. In historical institutionalism and evolutionary futures studies, institutional
42 change is often divided into periods of institutional stability and brief periods of rapid changes –
43 the so-called punctuated equilibrium model (Capoccia & Kelemen, 2007; Mannermaa, 1991). The
44 central idea is that institutions exhibit certain inertia but when they change, it is a sudden and
45 rapid event or sequence of events. Change is conceptualised as brief exceptional periods between
46 equilibria or as a result of exogenous shocks.

47
48 However, it is questionable whether the punctuated equilibrium model is suitable for explaining
49 changes in privacy protection. Mahoney & Thelen (2009) criticise the punctuated equilibrium
50 model for locating changes in great ruptures and thus failing to explain gradual endogenous
51 change. The authors define institutions as permanently fragile and contested settlements based

52
53 ⁸In understanding the motivations behind these actions, the insights of critical futures studies may prove
54 valuable. Critical futures studies may also be used to question who is portrayed as an actor.

1
2 on specific coalitional dynamics and with certain distributional effects. In other words, the
3 continuation of an institution requires active efforts. Even rapid changes may be the result of
4 latent long-term conflicts. According to Mahoney and Thelen, institutions are contestable because
5 institutional rules are always ambiguous to some extent and therefore they can be adapted to
6 each actor's purposes.
7

8 In this article, I will adopt this framework of contested institutions and gradual change. This
9 approach is more fruitful in studying privacy protection than the punctuated equilibrium model
10 for three reasons. Firstly, privacy protection has been a debated issue for decades and it is
11 difficult to discern periods of uncontested equilibrium (for a possible periodisation, see Westin,
12 2003). External shocks such as new technologies have influenced privacy debates, but their
13 impact has not necessarily been a rupture of the system. Secondly, institutional rules in privacy
14 protection are ambiguous, as C. J. Bennett & Raab (2006, p. 255, 285) highlight. Thirdly, the
15 framework makes it possible to understand conflicts of interest among actors. Contestation over
16 privacy protection is motivated by the contest over appropriate flows of information and over the
17 distribution of economic and power benefits gained through information. Since information is a
18 valuable commodity, it motivates actors to try to influence the rules of privacy protection.
19
20
21

22 **4. Three-stage framework for creating privacy protection scenarios**

23

24 How can the approach of institutional change be applied to studying futures of privacy protection?
25 In the following, I will argue that scenarios of plausible futures can be constructed based on
26 theoretical understanding of privacy dynamics and knowledge of historical processes. This can
27 be done using a framework with three stages: 1) outlining the dynamics of privacy protection,
28 2) tracing historical processes and formulating causal narratives, and 3) building event-based
29 scenarios. Each stage feeds into the next stage. The focus is on constructing scenarios with rigorous,
30 theoretically justifiable content. Other aspects of the scenario process, such as communicating
31 results to stakeholders, visioning of preferred futures and embedding scenario thinking into the
32 organisational context, are not addressed.
33

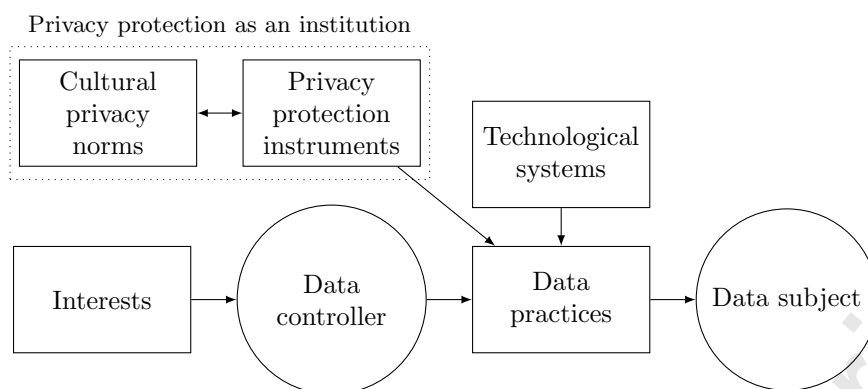
34 *4.1. Outlining the dynamics of privacy protection*

35 *4.1.1. The context of privacy protection*

36
37
38 The first step in studying futures of privacy is outlining the dynamics of privacy protection in
39 order to focus on factors relevant to its development over time. Privacy as such is a contextual
40 and situational phenomenon and analysing its development over time is extremely complex
41 (Nissenbaum, 2010; Solove, 2008). Thus the specific focus on privacy *protection* is beneficial
42 because then the inquiry can be directed at factors which influence institutionalised privacy rules
43 rather than all behaviour related to privacy.
44

45 Daniel Solove's (2008, p. 104) framework is a useful starting point in balancing between a
46 contextual and general understanding. The central point of Solove's framework is a relationship
47 between two actors: the data controller and the data subject. Building on this approach, I have
48 developed a heuristic model which puts the institution of privacy protection in context (Fig. 1).
49

50 The central part of this extended model is still the relationship between two actors depicted as
51 circles. In this relationship, the data controller collects, utilises and disseminates data about an
52 individual, the data subject. The data controller may be either an individual or, more likely, a
53
54
55
56
57
58
59
60
61
62
63
64
65



19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Figure 1: Privacy dynamics model

public or private organisation. I have added several mediating factors in this relationship: cultural norms, privacy protection instruments, technologies and interests.

The institution of privacy protection consists of cultural privacy norms and privacy protection instruments. The focus here is on the latter which comprises institutionalised instruments such as data protection legislation, data protection authorities, privacy commissioners and privacy standards. It can also be seen to encompass technological instruments such as encryption technologies.

The role of privacy protection instruments is the regulation of data-related practices in the relation between data controller and data subject (C. J. Bennett & Raab, 2006). Examples of privacy-violating practices include intrusion, data collection, unauthorised secondary use, improper access and combining data (Smith, Milberg, & Burke, 1996; Solove, 2008). I would argue that such practices are established by data controllers because they serve that actor's *interests*, be it governance, national security, profit or simply curiosity.⁹ For instance, trading in personal information online has become a lucrative business, and modern welfare states require extensive amounts of data to coordinate social benefits (Mayer-Schönberger, 1997; Nissenbaum, 2010). Interests are here understood as driving forces behind actions, and the concept should be seen broadly, encompassing not only economic self-interest but also political and social interests, for instance (Swedberg, 2005).

An interest-based account can be criticised for exaggerating the intentionality of actors, while in reality privacy violations may emerge as unintended consequences with no malicious intent (Nissenbaum, 2010, pp. 241–243; Solove, 2008, pp. 177–178, 187). The issue of intentionality cannot be discussed at length within the space of this article. For my purposes, it is enough to claim that actors rarely have the aim of diminishing individuals' privacy, but it can be a logical consequence of their other aims such as ensuring efficient provision of public services.

47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

⁹The argument that technologies united with interests threaten privacy has been made by Warren & Brandeis (1890), Westin (1967) and Gavison (1980). Regan (1995), in turn, argues that the interests of social organisations and issues of power imbalances have not been adequately examined in the literature on privacy.

4.1.2. Development over time

There is no single macro process which determines developments in privacy protection. There are several relevant areas of development, some of which are outlined in Fig. 2.

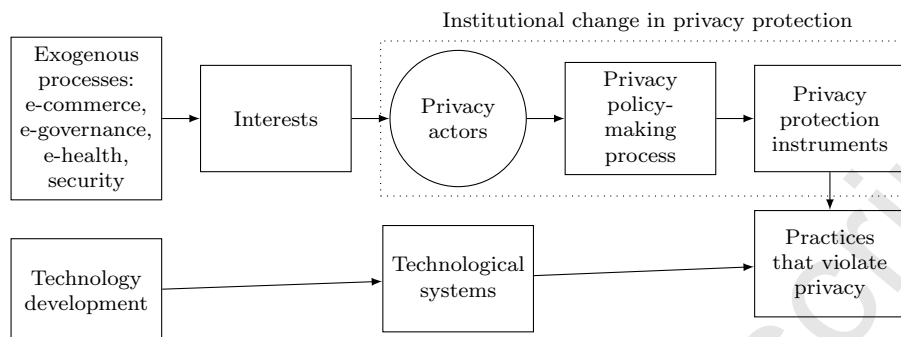


Figure 2: Processes which influence privacy protection

On the left-hand side of the figure, five broad exogenous processes are identified: the evolution of e-commerce, e-governance and e-health, developments in security and anti-terrorism, and technology development processes. Each of these areas may influence privacy protection, and many others could be added to the list. However, in the following, the focus is on the endogenous process of privacy policy-making for two reasons. Firstly, the aim of this article is to lower the level of abstraction from broad trends to sequences of events, and this requires a clear conceptual focus. Secondly, the external processes are brought into the privacy policy-making process. Security, commerce and governance contribute to the interests which motivate privacy-violating practices, while technology development in turn contributes to the technological systems which facilitate such violations.

Technology development deserves a special mention because it is often seen as a central driver of developments in privacy. Historically, concern over privacy has risen together with new technological possibilities (Gavison, 1980; Warren & Brandeis, 1890; Westin, 2003). Current privacy threats include tracking and monitoring technologies such as sensor networks, radio-frequency identification (RFID) tags, big data and social media sites (Lockton & Rosenberg, 2005; Nissenbaum, 2010, pt. 1). Emerging threats include ambient intelligence, the Internet of Things, Google Glass and the quantified self, as well as developments in nanotechnology, biotechnology and robotics (Arthur, 2013; De Hert et al., 2009; Economist, 2012; Hauptman & Katz, 2011, ch. 3; Mannermaa, 2007; Weber, 2010).

In privacy-related studies, there is a temptation to draw an arrow between developments in technology and the fate of privacy protection. Technological innovations seem to have a momentum that is difficult for policy to manage (C. J. Bennett & Raab, 2006, ch. 10). Nevertheless, to draw a line from new technologies to changes in privacy protection is too simple. Firstly, ‘technology’ encompasses multiple levels with different privacy implications, from generic technologies to technological artifacts and applications (Brey, 2012). Secondly, new digital technologies may also increase privacy and thus their net effect is unclear (Floridi, 2005). Most importantly, technology itself does not violate privacy. Violations occur when technologies are used in practices which violate privacy norms.¹⁰

¹⁰Even though it is not the focus of this article, technology design is an important domain because technological

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Privacy protection instruments are created and modified through the privacy policy-making process which involves numerous private and public actors, issue networks and policy communities. (C. J. Bennett & Raab, 2006; Regan, 1995, p. 19). Companies and interest groups continuously try to influence privacy legislation by lobbying for or against data protection proposals or by influencing the climate of opinion.

As Mahoney & Thelen (2009) point out, institutional rules are always somewhat ambiguous. Some practices are clearly in violation of norms, while others are more contestable. For example, filming one's neighbour's bedroom with a drone camera is a violation, but is bulk analysis of citizens' emails a violation if there is a demonstrable terrorist threat? Due to this ambiguity, actors continuously test the limits of privacy norms through practices, either intentionally or unintentionally. As a result of this continuous negotiation and testing, privacy protection instruments have their own trajectory of historical development, such as the different 'cultures of privacy' in the United States and Europe (Whitman, 2004).

In order to explain changes in privacy protection, privacy actors need to be conceptualised in a theoretically useful way. C. J. Bennett & Raab (2006, p. 220) recognise six roles that are involved in the negotiation over privacy protection: 1) regulatory bodies, 2) data controllers, 3) privacy pressure groups and media, 4) technology developers and providers, 5) data subjects and 6) government policy-makers. In addition, the theory of gradual institutional change presented by Mahoney & Thelen (2009) presents four types of institutional change agents: 1) insurrectionaries, 2) symbionts, 3) subversives and 4) opportunists. These refer to actors with different strategies of social change: insurrectionaries seek to displace institutions, subversives create gradual change through layering new rules on top of old ones, symbionts preserve formal rules but are not committed to renewing them, and finally opportunists convert existing rules to serve their interests.

In the analysis of historical development, these categorisations could be mapped onto each other and actors' dominant strategies could be analysed. For example, is a particular company as a data controller acting as a subversive, covertly seeking to shift the rules of privacy protection? Or are they acting opportunistically? Why have they adopted such strategies? In addition to analysis of single actors' strategies, the coalitional dynamics of actors should be studied over time.

4.2. *Tracing historical processes*

The second step in constructing privacy protection scenarios is empirically studying processes of institutional change. In the literature, there have been efforts at tracing historical changes in privacy protection on the macro level, focusing on broad sociopolitical processes (e.g. Flaherty, 1992; Mayer-Schönberger, 1997; Westin, 2003). The understanding of change processes would benefit from an explicit focus on events and a narrative mode of explanation (see section 3.2). Corresponding with this focus, the aim in this stage is to formulate a *causal narrative*, that is, a sequence of causally linked events that explains the crucial points in the change process (Mahoney, 2000b). The causal narrative concerns a *reactive sequence* of events, that is, a sequence in which each event is causally connected to prior events (Mahoney, 2000a).

Process tracing is an appropriate method for this purpose. According to Bengtsson & Ruonavaara (2011, p. 403), process tracing is "an attempt to reconstruct as closely as possible the chain of

lock-in means that technologies may have impacts far beyond their immediate applications, hence the recent focus on 'privacy by design' (Adam & Groves, 2007, p. 105; Hustinx, 2010; Perkins, 2003).

1
2
3 social mechanisms which leads from the situation at point A to the situation at point B". Process
4 tracing is particularly suited to studying social processes because it permits studying complex
5 causal relationships involving nonlinear dynamics, tipping points and equifinality (George &
6 Bennett, 2005; Reilly, 2010).

7
8 The first question is choosing the processes to study. Prominent privacy-related legislation
9 processes at the national or international level are obvious candidates. Then the causal process
10 needs to be broken down into smaller events for formulating a causal narrative. The key question
11 then is which events are central to the process. Historical institutionalists write about *critical*
12 *junctions*: relatively brief periods of increased agency when actors can influence a path-dependent
13 process (Capoccia & Kelemen, 2007). A critical juncture provides an opportunity to break a
14 path that has been established by path dependence (Tiberius, 2011). However, as was mentioned
15 above, Mahoney & Thelen (2009) argue that institutions tend to develop gradually through
16 continuous contestation of rules, and researchers have pointed out that path dependence is less
17 common than often assumed (Mahoney, 2000a; Vergne & Durand, 2010). Thus it is perhaps
18 more appropriate to consider critical events in the context of continuous negotiation rather than
19 adopting the binary notion of critical junctures and path-dependent processes.

20
21 In an institutional change process, a critical event can be defined as an event which is necessary
22 for defining the direction of a process. In order to identify critical events, counterfactual reasoning
23 is needed to discover historical alternatives that could have happened if a different decision were
24 taken at a key point (Aminzade, 1992; Capoccia & Kelemen, 2007, p. 354). Counterfactual
25 analysis also helps to specify the proposed causal mechanisms by asking what-if questions at
26 different points in the narrative chain (Durand & Vaara, 2009; Mahoney, 2000a). In addition to
27 counterfactual reasoning, the comparative case study approach can help to identify critical events
28 by comparing instances of the same phenomenon (George & Bennett, 2005).

29
30 An additional challenge in process tracing is generalisation. History does not repeat itself, but
31 similar patterns may be found in event sequences. Event structure analysis (ESA) is a central
32 method for generalising event sequences and discovering patterns. In ESA, the analyst constructs
33 a generalised representation of a sequence of events, continuously asking whether an event is
34 a necessary precondition for another event to occur (Griffin, 1993). Using this method, the
35 narrative data acquired through process tracing can be formalised and simplified into a skeleton
36 narrative which only includes essential events.

37 38 4.3. Building event-based scenarios

39
40 The final phase in the investigation is creating scenarios based on the understanding of privacy
41 dynamics and the patterns in causal narratives. Privacy scenarios created in this manner are
42 event-based rather than trend-based, focusing on actors, chains of events and discontinuity (Bishop
43 et al., 2007; Bruun, Hukkinen, & Eklund, 2002; Kahn & Wiener, 1967; Notten, Slegers, & Asselt,
44 2005). The construction of event-based scenarios can be likened to process tracing. The futures
45 researcher is considering chains of events and counterfactual possibilities, similar to counterfactual
46 history (Booth, Rowlinson, Clark, Delahaye, & Procter, 2009).

47
48 However, constructing scenarios of the future differs from historical analysis because there are
49 no uncontested future facts – the futures researcher is explaining potential but not actual
50 phenomena. Decisions leading to future outcomes are yet to be made and cannot be predicted
51 with certainty. Therefore the futures researcher can only make conjectures about causal chains
52 which may plausibly happen if certain decisions are made. This chain can be seen as a hypothetical
53 reactive sequence of actions and reactions, similar to the sequences identified through process
54

1
2 tracing (Notten, Rotmans, Asselt, & Rothman, 2003). However, scenarios are not purely works
3 of creative imagination, because theory and data about action-reaction mechanisms are used in
4 validating what-if claims.
5

6 In addition to historical knowledge, expert knowledge can be used to investigate plausible future
7 paths. The causal chains identified in the previous stage can be continued through the chains
8 of argumentation provided in expert interviews or in a Delphi process. Because the focus is on
9 constructing alternative future paths, a dissensus-based Delphi method, such as those presented by
10 Kuusi (1999) and Tapio (2003), is appropriate. It is also crucial to connect the expert arguments
11 with the historical data and theoretical hypotheses.
12

13 For event-based scenarios, the future may be visualised as a branching tree with nodes denoting
14 key events or decision points. In this model, the future may be seen as branching infinitely: each
15 decision could be made differently, thus leading to a cascade of different outcomes. The previous
16 scenario steps help to discern relevant events which create futures that are different in non-trivial
17 ways.
18

19 Similarly to event structure analysis, scenarios should focus only on the key actors and events,
20 and the what-if assumptions about future events and actions should be kept simple and explicit.
21 This is important because the scenario is structured as a reactive sequence in which each event
22 depends on the prior ones (Mahoney, 2000a). If one of the links is weak, the subsequent links
23 are also called into question. Therefore, scenarios should be analytical skeleton narratives which
24 ignore much of the contextual detail. This differs from typical scenario building where scenarios
25 are often vivid descriptions of future societal conditions.
26

27 Because decisions leading to future outcomes are yet to be made, the notions of tractability and
28 agency are central in futures studies (Malaska, 2001). Jouvenel (1967, pp. 52–53) distinguishes
29 between *masterable futures* which can be influenced and *dominating futures* which cannot be
30 influenced, arguing that the boundary between masterable and dominating depends on the power
31 of the actor in question. In institutional analysis, actors can be divided into rule makers and rule
32 takers (Streeck & Thelen, 2005). Taking into consideration Mahoney and Thelen's (2009) notions
33 of ambiguous rules and continuous negotiation, we can conceptualise agency as a continuum:
34 some actors are closer to *future makers*, both as rule makers and being able to interpret rules to
35 their benefit. Other actors are more akin to *future takers* bound by rules they cannot influence.
36

37 The focus on temporal sequences adds the element of timing, since the possibility of influencing
38 the future depends on the point in time in the continuous negotiation over privacy protection.
39 Thus the roles of future makers and future takers change over time. Tiberius (2011) refers to
40 three phases in path-dependent processes: preformation phase, formation phase and lock-in phase.
41 In the beginning outcomes are highly uncertain, the middle phase is the critical juncture and the
42 final phase represents a deterministic process marked by path dependence. In other words, both
43 uncertainty and agency decrease over time in path-dependent processes.
44

45 The analysis of power and agency contributes to an important goal of scenario building: identifying
46 leverage points in institutional change processes (Meadows, 1999). If an undesirable path is in
47 sight, how could the path be broken and who could break it? Which actors can act as future
48 makers in the privacy policy process? In the context of event sequences, a leverage point refers to
49 two things: an aspect of the system, such as actors and incentives, and a point in time. This
50 raises questions about ethics and perspective (undesirable future for whom?), and critical and
51 participatory methods may be useful in providing answers.
52

53 Constructing scenarios is beyond the scope of this article, but as an illustration, we can consider
54 the current debate on the so-called *right to be forgotten*. This debate is centred on the question
55
56

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

whether citizens of EU countries have the right to ask search engine providers to remove outdated or stigmatising search engine results that include their names (Mantelero, 2013). According to the privacy dynamics model outlined in section 4.1.1, the debate concerns the practices of data controllers, which are influenced by technological factors such as the distribution of search engines across different country domains. The key actors include Google (a data controller), the European Parliament, Council and Commission (government policy-makers), the European Court of Justice, data protection authorities and the Article 29 Working Party (regulators), as well as media and civil society. As exogenous processes, we can consider the ongoing transnational trade negotiations which are likely to influence data protection, and also the terror attacks in New York, Madrid and London in the early 2000s which led to security issues climbing on the agenda and to the surveillance practices revealed by Edward Snowden.

The second step, process tracing, would require a close analysis of the steps in the sequence and the mechanisms that connect them. Key events include the original complaint about search results made in 2010 by a Spanish man, the May 2014 ruling of the European Court of Justice on the right to ask for removal of search results, the subsequent launch of Google's Advisory Council, and negotiation between the European Parliament, Council and Commission over the General Data Protection Regulation which is ongoing at the time of writing. The question of mechanisms demands closer social scientific scrutiny. For instance, what is the role of pressure from media and civil society on the actions of the data controller? What are the strategic interests of actors related to data protection and how have they advanced them? What kind of alliances have been formed at different points in time?

Finally, scenarios could be built as a continuation of this process. In one hypothetical scenario, the right to be forgotten is widely instituted, leading to reactions from data controllers and possibly pressure for more comprehensive data protection also outside Europe. In another hypothetical scenario, the right to be forgotten is dropped because data controllers and policy-makers reach an agreement that the Internet should be minimally regulated. In this case, these actors act together as future makers. This could lead to diverging reactions from companies, media and civil society. In constructing such scenarios, it is important to find a balance between considering the concrete historical sequence and making conditional and justifiable generalisations. This brief illustration also suggests the question whether the debate over the right to be forgotten is a leverage point in influencing privacy protection more widely.

This scenario approach has two potential weaknesses: assumptions about the stability of underlying mechanisms and relatively short time horizon. The framework relies on the assumption that types of event sequences that occurred in the past could also occur in the future. If the causal links in the event sequence can be generalised through event structure analysis, for example, they may plausibly also hold in the future (Abell, 2004, p. 295). Such forecasting needs to be done cautiously because mechanisms in open systems produce tendencies rather than universal laws, and outcomes are always caused by many interacting mechanisms (Bhaskar, 1998, p. 10, 23; Elder-Vass, 2010, p. 47; Hedström & Ylikoski, 2010). Thus for instance privacy legislation may lead to stricter adherence to privacy norms, but this influence may be altered by decisions taken by an influential data controller. A related issue is that long-range scenarios cannot be created with this approach, because uncertainty increases as one moves further into the future. If one is considering a time frame of many decades, the amount of events and branching points becomes overwhelming, and it is difficult to argue for a limited number of scenarios.

Despite these limitations, this scenario approach has several benefits in comparison to more traditional scenario methods in creating issue-based scenarios. It is based on a clear conceptual focus on privacy protection as a social institution and on the process of gradual institutional

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

change. This conceptual focus allows making well-grounded conjectures about which actors and events may influence the development of privacy protection. The focus on events and mechanisms gives a sounder basis to conjectures about the future than trend extrapolation. Specific future events cannot be predicted, but it is possible to make plausible conjectures about types of event sequences. Even if event sequences will not necessarily be repeated, they represent a more profound understanding of change processes than trend extrapolation, because hypotheses about background factors are made explicit (Bergman, Karlsson, & Axelsson, 2010).

On a more abstract level, the focus on mechanisms and event sequences allows a middle path between the future as the continuation of trends and the future as radically discontinuous. Mechanisms are not universal laws, but one can assume that similar mechanisms are likely to produce similar outcomes in similar contexts. Thus scenarios as event sequences can be a logical continuum from the past even if they are not a continuation of past trends.

5. Conclusion

This article focused on the question how futures of privacy protection can be studied using scenario methodology. In answer to this question, a framework for constructing privacy scenarios was presented. First previous definitions of privacy and studies on the futures of privacy were described and their shortcomings were highlighted. The point was not to argue that previous scenario analysts have been mistaken, but that the intention in this article is different: to analyse plausible futures of privacy protection from a social science perspective.

For this purpose, the focus was placed on privacy *protection*, defined as a social institution which encompasses laws and cultural norms. The article proposed an institutional change framework, in particular the approach of gradual institutional change, for studying futures of privacy protection. I have argued that a focus on sequences of events is beneficial in this task.

In practice, futures of privacy protection may be studied using a three-stage framework. The stages are 1) outlining the dynamics of privacy protection, 2) studying historical processes and formulating causal narratives and 3) building event-based scenarios that describe potential chains of events. The general pattern of moving from understanding systems and history to outlining possible futures is familiar from standard foresight methods as well as approaches such as six pillars and the Manoa School method (Bishop et al., 2007; Dator, 2009; Inayatullah, 2008), but this article suggests conceptual tools that are suitable for studying institutional change. In order to explain the dynamics of privacy, I have presented a heuristic model which includes actors, practices, technological systems and privacy protection instruments. Process tracing and event structure analysis were identified as appropriate methods for investigating historical changes in privacy protection. Finally, event-based scenarios should be built based on identified patterns of actions and events. In this effort, the framework of dominating and masterable futures is useful.

The framework provides many benefits for futures research of privacy and of social institutions more generally. Firstly, the framework helps to understand the complex dynamics of privacy protection on a more concrete level than previous studies which have examined macro-level trends. Once institutional changes in privacy protection are better understood, it is possible to outline plausible future paths if certain events take place.

However, scenarios of the future of privacy ultimately need to be brought back to the level of present planning and decision-making. The goal of scenario building is to identify leverage points. If the future of privacy is going in an undesirable direction, how has this happened and what could be done to prevent it? Which actors have the power to influence the process? Which policy

1
2 mechanisms are available for redirecting the process and when should they be applied? The
3 knowledge of causal mechanisms and possible event sequences provides a basis for proactively
4 intervening in processes, promoting desirable outcomes and preventing undesirable ones.
5

6 The framework presented in the article could be adapted to studying other social institutions such
7 as intellectual property or wage labour. If the phenomena are similar enough, the mechanisms of
8 institutional change are likely to be similar, and therefore the focus on dynamics, historical process
9 tracing and scenario construction is likely to be fruitful across many different cases. However,
10 the actors, institutional properties and environmental factors are different, which means that the
11 details of the framework need to be adapted in each case.
12

13 The substantive implication of the approach taken in the article is that the future of privacy is
14 not determined by any technological or other trend. However, equally importantly, the future of
15 privacy is not purely the product of imagination and visioning. Privacy protection is a social
16 institution with a particular history and dynamics, and it is important to understand these
17 when making statements about possible futures of privacy and when attempting to influence
18 institutional change.
19

20 21 Acknowledgements

22 I wish to thank Aino Halinen-Kaila for making me consider the conceptual focus, Petri Tapio,
23 Sirkka Heinonen and two anonymous reviewers for comments on earlier versions, and Burkhard
24 Auffermann for support and guidance. The research was funded by the Turku University
25 Foundation and the University of Turku Graduate School. The funders had no involvement in
26 the content of the research.
27
28
29

30 31 References

- 32
33
34 6, P. (1998). *The future of privacy*. London: Demos.
- 35 Abell, P. (2004). Narrative explanation: An alternative to variable-centered explanation? *Annual*
36 *Review of Sociology*, 30(1), 287–310. <http://doi.org/10.1146/annurev.soc.29.010202.100113>
- 37 Adam, B., & Groves, C. (2007). *Future Matters: Action, Knowledge, Ethics*. Leiden: Brill.
- 38 Ahonen, P., Alahuhta, P., Daskala, B., Delaitre, S., Hert, P. D., Lindner, R., . . . Verlinden, M.
39 (2010). Dark scenarios. In D. Wright, M. Friedewald, Y. Punie, S. Gutwirth, & E. Vildjiounaite
40 (Eds.), *Safeguards in a World of Ambient Intelligence* (pp. 33–142). Springer Netherlands.
41 http://doi.org/10.1007/978-1-4020-6662-7_3
- 42 Aminzade, R. (1992). Historical Sociology and Time. *Sociological Methods & Research*, 20(4),
43 456–480. <http://doi.org/10.1177/0049124192020004003>
- 44 Arthur, C. (2013, June). Google Glass: is it a threat to our privacy? Retrieved from <http://www.guardian.co.uk/technology/2013/mar/06/google-glass-threat-to-our-privacy>
45
46
- 47 Auffermann, B., Luoto, L., Lonkila, A., & Vartio, E. (2012, February). PRACTIS Deliverable 4.2:
48 Report on potential changes in privacy climates and their impacts on ethical approaches.
49
- 50 Baghai, K. (2012). Privacy as a Human Right: A Sociological Theory. *Sociology*, 46(5), 951–965.
51 <http://doi.org/10.1177/0038038512450804>
52
53
54
55

- 1
2 Barkey, K. (2009). Historical Sociology. In P. Hedström & P. S. Bearman (Eds.), *The Oxford*
3 *handbook of analytical sociology* (pp. 712–733). Oxford: Oxford University Press.
4
- 5 Bell, W. (1997). *Foundations of Futures Studies: Human Science for a New Era. Vol. 1, History,*
6 *Purposes and Knowledge.* New Brunswick, N.J.: Transaction Publishers.
7
- 8 Bengtsson, B., & Ruonavaara, H. (2011). Comparative Process Tracing in Housing Studies.
9 *International Journal of Housing Policy, 11*(4), 395–414. [http://doi.org/10.1080/14616718.2011.](http://doi.org/10.1080/14616718.2011.626603)
10 626603
- 11 Benn, S. I. (1971). Privacy, freedom, and respect for persons. *Nomos XIII: Privacy.* Atherton
12 *Press, New York.*
13
- 14 Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global*
15 *Perspective.* Cambridge, Mass.: MIT Press.
16
- 17 Bergman, A., Karlsson, J. C., & Axelsson, J. (2010). Truth claims and explanatory claims—An
18 ontological typology of futures studies. *Futures, 42*(8), 857–865. [http://doi.org/10.1016/j.futures.](http://doi.org/10.1016/j.futures.2010.02.003)
19 2010.02.003
- 20 Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information
21 Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017–A36.
22
- 23 Bhaskar, R. (1998). *The Possibility of Naturalism: A Philosophical Critique of the Contemporary*
24 *Human Sciences* (3rd ed.). London: Routledge.
25
- 26 Bishop, P., Hines, A., & Collins, T. (2007). The current state of scenario development: an
27 overview of techniques. *Foresight, 9*(1), 5–25. <http://doi.org/10.1108/14636680710727516>
- 28 Bloustein, E. J. (1964). Privacy as an aspect of human dignity: an answer to Dean Prosser. *New*
29 *York University Law Review, 39,* 962–1007.
30
- 31 Booth, C., Rowlinson, M., Clark, P., Delahaye, A., & Procter, S. (2009). Scenarios and counter-
32 factuals as modal narratives. *Futures, 41*(2), 87–95. <http://doi.org/10.1016/j.futures.2008.07.037>
- 33
34 Bradfield, R., Wright, G., Burt, G., Cairns, G., & Van Der Heijden, K. (2005). The origins
35 and evolution of scenario techniques in long range business planning. *Futures, 37*(8), 795–812.
36 <http://doi.org/10.1016/j.futures.2005.01.003>
- 37 Brey, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. *NanoEthics, 6*(1), 1–13.
38 <http://doi.org/10.1007/s11569-012-0141-7>
39
- 40 Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy*
41 *and Freedom?* Reading, Mass.: Perseus Books.
42
- 43 Bruun, H., Hukkinen, J., & Eklund, E. (2002). Scenarios for coping with contingency: The case
44 of aquaculture in the Finnish Archipelago Sea. *Technological Forecasting and Social Change,*
45 *69*(2), 107–127. [http://doi.org/10.1016/S0040-1625\(01\)00134-2](http://doi.org/10.1016/S0040-1625(01)00134-2)
- 46 Capoccia, G., & Kelemen, R. D. (2007). The study of critical junctures: Theory, narrative, and
47 counterfactuals in historical institutionalism. *World Politics, 59*(03), 341–369. Retrieved from
48 http://journals.cambridge.org/abstract_S0043887100020852
49
- 50 Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday*
51 *Practice.* New Haven Conn.: Yale University Press.
52
- 53 Dator, J. (2009). Alternative futures at the Manoa school. *Journal of Futures Studies, 14*(2),
54 1–18.
55

- 1
2
3 De Hert, P., Gutwirth, S., Moscirobroda, A., Wright, D., & González Fuster, G. (2009). Legal
4 safeguards for privacy and data protection in ambient intelligence. *Personal and Ubiquitous*
5 *Computing*, 13(6), 435–444. <http://doi.org/10.1007/s00779-008-0211-6>
- 6 DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca:
7 Cornell University Press.
- 8 Durand, R., & Vaara, E. (2009). Causation, counterfactuals, and competitive advantage. *Strategic*
9 *Management Journal*, 30(12), 1245–1264. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true/&db=bth/&AN=44540803/&site=ehost-live>
- 10 Economist. (2012, March). The quantified self: Counting every moment. Retrieved from
11 <http://www.economist.com/node/21548493>
- 12 Elder-Vass, D. (2010). *The Causal Power of Social Structures: Emergence, Structure and Agency*.
13 Cambridge ; New York: Cambridge University Press.
- 14 Flaherty, D. H. (1992). *Protecting Privacy in Surveillance Societies: The Federal Republic of*
15 *Germany, Sweden, France, Canada, and the United States*. University of North Carolina Press.
- 16 Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Informa-*
17 *tion Technology*, 7(4), 185–200. <http://doi.org/10.1007/s10676-006-0001-7>
- 18 Fried, C. (1968). Privacy. *Yale Law Journal*, 77(3), 475–493.
- 19 Fuchs, C. (2011). An Alternative View of Privacy on Facebook. *Information*, 2(4), 140–165.
20 <http://doi.org/10.3390/info2010140>
- 21 Gavison, R. (1980). Privacy and the Limits of Law. *Yale Law Journal*, 89(3), 421–471. <http://doi.org/10.2307/795891>
- 22 George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*.
23 Cambridge, Mass.: MIT Press.
- 24 Griffin, L. J. (1993). Narrative, Event-Structure Analysis, and Causal Interpretation in Historical
25 Sociology. *American Journal of Sociology*, 98(5), 1094–1133. Retrieved from <http://www.jstor.org/stable/2781584>
- 26 Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of*
27 *Sociology*, 51(4), 605–622. <http://doi.org/10.1080/00071310020015280>
- 28 Hauptman, A., & Katz, O. (2011, July). PRACTIS Deliverable 2.2: Final Horizon Scanning
29 Report. Retrieved from http://www.practis.org/docs/PRACTIS/%20D2/%202_130711final.pdf
- 30 Hedström, P., & Ylikoski, P. (2010). Causal mechanisms in the social sciences. *Annual Review of*
31 *Sociology*, 36(1), 49–67. <http://doi.org/10.1146/annurev.soc.012809.102632>
- 32 Henning, C. (2007). Institution. In G. Ritzer (Ed.), *Blackwell Encyclopedia of Sociology*. Blackwell
33 Reference Online. Retrieved from http://www.blackwellreference.com/subscriber/tocnode.html?id=g9781405124331_chunk_g978140512433115_ss1-50
- 34 Höjer, M., & Mattsson, L.-G. (2000). Determinism and backcasting in future studies. *Futures*,
35 32(7), 613–634. [http://doi.org/10.1016/S0016-3287\(00\)00012-4](http://doi.org/10.1016/S0016-3287(00)00012-4)
- 36 Hustinx, P. (2010). Privacy by design: delivering the promises. *Identity in the Information*
37 *Society*, 3(2), 253–255. <http://doi.org/10.1007/s12394-010-0061-z>
- 38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

1
2
3 Inayatullah, S. (2002). Reductionism or layered complexity? The futures of futures stud-
4 ies. *Futures*, 34(3), 295–302. Retrieved from [http://www.sciencedirect.com/science/article/pii/](http://www.sciencedirect.com/science/article/pii/S0016328701000453)
5 S0016328701000453

6 Inayatullah, S. (2004). Deconstructing and reconstructing the future: predictive, cultural and
7 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:
8 Tamkang University Press.

9
10 Inayatullah, S. (2008). Six pillars: futures thinking for transforming. *Foresight*, 10(1), 4–21.

11
12 Jouvenel, B. de. (1967). *The Art of Conjecture*. New York: Basic Books.

13
14 Kahn, H., & Wiener, A. J. (1967). *The year 2000: a framework for speculation on the next*
15 *thirty-three years*. Macmillan New York.

16
17 Kaivo-oja, J. Y., Katko, T. S., & Seppälä, O. T. (2004). Seeking convergence between history
18 and futures research. *Futures*, 36(5), 527–547. <http://doi.org/10.1016/j.futures.2003.10.017>

19
20 Kuusi, O. (1999). *Expertise in the Future Use of Generic Technologies: Epistemic and Methodolog-*
21 *ical Considerations Concerning Delphi Studies*. Helsinki: Helsinki School of Economics; Business
22 Administration.

23
24 Lockton, V., & Rosenberg, R. S. (2005). RFID: The Next Serious Threat to Privacy. *Ethics and*
25 *Information Technology*, 7(4), 221–231. <http://doi.org/10.1007/s10676-006-0014-2>

26
27 Mahoney, J. (2000a). Path dependence in historical sociology. *Theory and Society*, 29(4), 507–548.
28 <http://doi.org/10.1023/A:1007113830879>

29
30 Mahoney, J. (2000b). Strategies of Causal Inference in Small-N Analysis. *Sociological Methods &*
31 *Research*, 28(4), 387–424. <http://doi.org/10.1177/0049124100028004001>

32
33 Mahoney, J., & Thelen, K. (2009). A Theory of Gradual Institutional Change. In *Explain-*
34 *ing Institutional Change* (pp. 1–37). Cambridge University Press. [http://doi.org/10.1017/](http://doi.org/10.1017/CBO9780511806414.003)
35 CBO9780511806414.003

36
37 Malaska, P. (2001). A futures research outline of a post-modern idea of progress. *Futures*, 33(34),
38 225–243. [http://doi.org/10.1016/S0016-3287\(00\)00069-0](http://doi.org/10.1016/S0016-3287(00)00069-0)

39
40 Mannermaa, M. (1991). In search of an evolutionary paradigm for futures research. *Futures*,
41 23(4), 349–372.

42
43 Mannermaa, M. (2007). Living in the European ubiquitous society. *Journal of Futures Studies*,
44 11(4), 105–120.

45
46 Mannermaa, M. (2008). *Jokuveli: elämä ja vaikuttaminen ubiikkiyhteiskunnassa*. Helsinki:
47 WSOYpro.

48
49 Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the
50 roots of the “right to be forgotten”. *Computer Law & Security Review*, 29(3), 229–235. <http://doi.org/10.1016/j.clsr.2013.03.010>

51
52 Manzo, G. (2007). Comment on Andrew Abbott. *Sociologica*, 1(2), 1–8.

53
54 Masini, E. B. (2010). The past and the possible futures of Futures Studies: Some thoughts on
55 Ziauddin Sardar’s “the namesake”. *Futures*, 42(3), 185–189. [http://doi.org/10.1016/j.futures.](http://doi.org/10.1016/j.futures.2009.11.002)
56 2009.11.002

- 1
2
3 Mayer-Schönberger, V. (1997). Generational development of data protection in Europe. In P.
4 E. Agre & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (pp. 219–241).
5 Cambridge, MA, USA: MIT Press.
- 6
7 Meadows, D. H. (1999). Leverage Points: Places to Intervene in a System. The Sustainability
8 Institute; The Sustainability Institute; The Sustainability Institute. Retrieved from http://www.donellameadows.org/wp-content/userfiles/Leverage_Points.pdf
9
- 10
11 Moore, B. (1984). *Privacy: studies in social and cultural history*. Armonk, N.Y: Sharpe.
- 12
13 Nissenbaum, H. F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social
Life*. Stanford, Calif.: Stanford Law Books.
- 14
15 Notten, P. W. F. van, Rotmans, J., Asselt, M. B. A. van, & Rothman, D. S. (2003). An updated
16 scenario typology. *Futures*, 35(5), 423–443. [http://doi.org/10.1016/S0016-3287\(02\)00090-3](http://doi.org/10.1016/S0016-3287(02)00090-3)
- 17
18 Notten, P. W. F. van, Slegers, A. M., & Asselt, M. B. A. van. (2005). The future shocks: On
19 discontinuity and scenario development. *Technological Forecasting and Social Change*, 72(2),
20 175–194. <http://doi.org/10.1016/j.techfore.2003.12.003>
- 21
22 Perkins, R. (2003). Technological “lock-in”. In *Online Encyclopaedia of Ecological Economics*.
Retrieved from <http://isecoeco.org/pdf/techlkin.pdf>
- 23
24 Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of
New York Press.
- 25
26 Pew Research Center. (2014). *The Future of Privacy*. Pew Research Center. Retrieved from
27 <http://www.pewinternet.org/2014/12/18/future-of-privacy/>
- 28
29 Poli, R. (2011). Steps toward an explicit ontology of the future. *Journal of Futures Studies*, 16(1),
30 67–78. Retrieved from http://www.academia.edu/download/31039228/2011_Poli_Steps.pdf
- 31
32 Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 4(4), 323–333.
- 33
34 Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel
Hill: University of North Carolina Press.
- 35
36 Reilly, R. C. (2010). Process Tracing. In A. J. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia
of Case Study Research* (pp. 735–737). Thousand Oaks, Calif.: SAGE Publications, Inc.
- 37
38 Reiman, J. H. (1976). Privacy, intimacy and personhood. *Philosophy & Public Affairs*, 6(1),
39 26–44.
- 40
41 Ritzer, G. (2001). Toward an integrated sociological paradigm: image of the subject matter. In
42 *Explorations in Social Theory: From Metatheorizing to Rationalization* (pp. 79–99). London:
43 SAGE.
- 44
45 Schoeman, F. D. (1992). *Privacy and Social Freedom*. Cambridge: Cambridge University Press.
- 46
47 Schwartz, P. (1996). *The Art of the Long View: Paths to Strategic Insight for Yourself and Your
Company*. New York: Currency Doubleday.
- 48
49 Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary
50 Review. *MIS Quarterly*, 35(4), 980–A27.
- 51
52 Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals’
53 concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. <http://doi.org/10.2307/249477>
54
55

- 1
2 Solove, D. J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.
3
4 Staley, D. J. (2007). *History and future: using historical thinking to imagine the future*. Lanham,
5 MD: Lexington Books.
6
7 Steeves, V. (2009). Reclaiming the social value of privacy. In I. Kerr, V. Steeves, & C. Lucock
8 (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*
9 (pp. 191–208). Oxford: Oxford University Press.
10
11 Streeck, W., & Thelen, K. (2005). Introduction: institutional change in advanced political
12 economies. In W. Streeck & K. Thelen (Eds.), *Beyond Continuity: Institutional Change in*
13 *Advanced Political Economies* (pp. 1–39). Oxford: Oxford University Press.
14
15 Swedberg, R. (2005). *Interest*. Maidenhead: Open University Press.
16
17 Tapio, P. (2003). Disaggregative policy Delphi: Using cluster analysis as a tool for systematic
18 scenario formation. *Technological Forecasting and Social Change*, 70(1), 83–101. Retrieved from
19 <http://linkinghub.elsevier.com/retrieve/pii/S0040162501001779>
20
21 Tavani, H. T. (2008a). Floridi's ontological theory of informational privacy: Some implications
22 and challenges. *Ethics and Information Technology*, 10(2-3), 155–166.
23
24 Tavani, H. T. (2008b). Informational privacy: concepts, theories, and controversies. In K. E.
25 Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 131–164).
26 Hoboken, N.J.: Wiley.
27
28 Thelen, K. (1999). Historical Institutionalism in Comparative Politics. *Annual Review of Political*
29 *Science*, 2(1), 369–404. <http://doi.org/10.1146/annurev.polisci.2.1.369>
30
31 Tiberius, V. (2011). Towards a “Planned Path Emergence” View on Future Genesis. *Journal of*
32 *Futures Studies*, 15(4), 9–24. Retrieved from <http://www.jfs.tku.edu.tw/15-4/A02.pdf>
33
34 Toor, A. (2015, January). Charlie Hebdo attacks raise fears of a European Patriot Act. *The*
35 *Verge*. Retrieved from [http://www.theverge.com/2015/1/14/7544537/charlie-hebdo-terrorist-](http://www.theverge.com/2015/1/14/7544537/charlie-hebdo-terrorist-attack-europe-patriot-act-surveillance)
36 [attack-europe-patriot-act-surveillance](http://www.theverge.com/2015/1/14/7544537/charlie-hebdo-terrorist-attack-europe-patriot-act-surveillance)
37
38 Vergne, J.-P., & Durand, R. (2010). The Missing Link Between the Theory and Empirics of
39 Path Dependence: Conceptual Clarification, Testability Issue, and Methodological Implications.
40 *Journal of Management Studies*, 47(4), 736–759. <http://doi.org/10.1111/j.1467-6486.2010.00913.x>
41
42 Von Drehle, D. (2013, August). The Surveillance Society. *Time*. Retrieved from [http://nation.](http://nation.time.com/2013/08/01/the-surveillance-society/)
43 [time.com/2013/08/01/the-surveillance-society/](http://nation.time.com/2013/08/01/the-surveillance-society/)
44
45 Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5),
46 193–220.
47
48 Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law*
49 *& Security Review*, 26(1), 23–30. Retrieved from [http://linkinghub.elsevier.com/retrieve/pii/](http://linkinghub.elsevier.com/retrieve/pii/S0267364909001939)
50 [S0267364909001939](http://linkinghub.elsevier.com/retrieve/pii/S0267364909001939)
51
52 Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.
53
54 Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2),
55 431–453. <http://doi.org/10.1111/1540-4560.00072>
56
57 Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale*
58 *Law Journal*, 113(6), 1151–1221. <http://doi.org/10.2307/4135723>
59
60
61
62
63
64
65

1
2
3 Wilkinson, A., Kupers, R., & Mangalagiu, D. (2013). How plausibility-based scenario practices
4 are grappling with complexity to appreciate and address 21st century challenges. *Technological*
5 *Forecasting and Social Change*, 80(4), 699–710. <http://doi.org/10.1016/j.techfore.2012.10.031>
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65

Figure

Institutional change in privacy protection

