

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Tiainen, Minna Katriina

Title: Negotiating digital surveillance legislation in post-Snowden times : An argumentation analysis of Finnish political discourse

Year: 2019

Version: Accepted version (Final draft)

Copyright: © John Benjamins Publishing Company

Rights: In Copyright

Rights url: <http://rightsstatements.org/page/InC/1.0/?language=en>

Please cite the original version:

Tiainen, M. K. (2019). Negotiating digital surveillance legislation in post-Snowden times : An argumentation analysis of Finnish political discourse. *Journal of Language and Politics*, 18(2), 207-230. <https://doi.org/10.1075/jlp.18004.tia>

Negotiating digital surveillance legislation in post-Snowden times: An argumentation analysis of Finnish political discourse

Minna Tiainen

In the digital era, when security agencies world-wide have been challenging basic democratic principles with massive data gathering, Finland has had a different approach: it has conducted no large-scale surveillance of citizens' online activities. Now, however, the country is planning such a vast expansion of state surveillance that the constitution itself must be altered. The present article examines one key point in this legislative process to see how the new surveillance measures are argued for and criticized, and how the differing points of view are negotiated to ultimately enable political action. Drawing particularly on Fairclough and Fairclough's (2012) approach to argumentation in political discourse, the article finds that surveillance is promoted as essential for national security, and criticized especially for its economic risks, consequences for civil rights and questionable effectiveness. Despite this range of critical perspectives, only economic considerations have become a topic of extended deliberation.

Key words:

Digital surveillance, political discourse, critical discourse studies, argumentation, privacy

1. Introduction

In the digital era, security agencies world-wide are searching through massive amounts of personal data from citizens not suspected of any crime. Information that was considered deeply private in the analogue world is gathered and processed unbeknown to the people concerned for reasons that are vaguely formulated and often difficult to verify. This has altered the societal status of civil rights such as privacy and, ultimately, the relationship between citizen and state (cf. e.g. Lyon 2015; Lyon 1994).

Among western democracies which develop and extensively utilize digital technology, Finland has constituted an exception: a country not conducting large-scale surveillance of digital activities, with intelligence legislation broadly considered outdated. Now, however, Finnish policymakers hope to update this legislation to address concerns relating to digitalization, taking heed of countries further along this path (more in Section 6). Their ultimate aim is such a massive expansion of state surveillance that changes to the constitution are needed. In a country that prides itself on respect for civil rights, the negotiation of these changes is an interesting topic for analysis.

The Finnish process is also topical because it coincides with the surge in global awareness of digital privacy that followed the 2013 Edward Snowden revelations. Demonstrating the unexpected extent of surveillance by the USA (among others), these revelations made the justification of surveillance an international topic of debate (e.g. Lyon 2015) and underlined how images of threat had been used to enable exceptional security measures (and continued to be used after the revelations; see e.g. Schulze 2015 and Tréguer 2017 on *securitization*; cf. justifications for the Finnish reform in Section 6). Subsequent political reforms have in places increased legal surveillance measures and in others constricted them (e.g. Hintz and Brown 2017, p. 789), prompting researchers both to credit Snowden with enhancing privacy protections (e.g. Ni Loideain 2015) and to trace how global outrage coincides with, or paradoxically even translates into, ever-broadening surveillance mandates (e.g. Tréguer 2017; Steiger et al. 2017). The present article sheds further light on the way the latter kind of development may take place.

This article examines how, during the ongoing Finnish legislative process, the changes are argued for and criticized and the differing perspectives negotiated to ultimately enable political action. Specifically, for the justifications for surveillance the article analyses a working group report commissioned by the Ministry of Defence, drafted at the height of the Snowden discussion. This report forms the basis for further legislative development, presenting a moment when the entirety of the proposed intelligence capabilities, as well as measures relevant for enabling them, are discussed together before being divided between different ministries (more in Section 2.2.). This report can therefore be considered a key point in the legislative process (cf. e.g. nexus in Scollon and Scollon 2004). For criticism and concerns over the proposals, the article analyses two of the report's appendices, which voice concerns regarding the suggested measures. This critique offers an interesting object of analysis both because it expresses a range of concerns typical of post-Snowden public discussion (more below) and because it was specifically expressed during, and as part of, the drafting of the working group report. This makes the treatment of this particular critique in the report itself especially revealing of the ways that different concerns about surveillance are addressed (or disregarded) in the legislative process.

For theoretical background, this article draws on surveillance studies (e.g. Lyon 2015; Mathiesen 2013; see also e.g. Haggerty and Ericson 2000 and Foucault 1977) for an understanding of the societal role of surveillance, and critical discourse studies (e.g. Wodak and Meyer 2016; Pietikäinen and Mäntynen 2009; Fairclough 1992; Jokinen 1999), particularly Fairclough and Fairclough (2012), for insights into political discussion. Taking a deliberative view of politics, Fairclough and Fairclough (*ibid.*) state that the main purpose of political language use is justifying particular action; therefore, it is fundamentally argumentative. The applicability of this view to all political discourse is controversial (see e.g. Hay 2013), but it fits the present data and is therefore useful in the selection of analytical tools here. The main analytical concept in this article is *argument*, understood as a speech act that concentrates on justifying a claim (*ibid.*, 35–38). The particular argument of interest in the working group report is one which advocates digital surveillance. This argument is first reconstructed to its claim and premises, after which the appendices are analysed for the ways they question it. Lastly, the way the critique is addressed and negotiated in the report itself is examined.

2. Digital surveillance and the case of Finland

2.1. Surveillance in the digital age

Surveillance can broadly be understood as “collecting information in order to manage or control” (Lyon 2015, 3; cf. Mathiesen 2013, 17). Its relevance for societies and individuals has long been acknowledged (see e.g. Foucault 1977), but recent social and technological developments have rendered it particularly topical. Thanks to digitalization, the pool of personal information easily available (and combinable) for different surveillance actors has vastly expanded, contributing to surveillance becoming more intensive, inexpensive and invisible than before (see e.g. Lyon 2014; Mathiesen 2013; Marx 2000). Widespread cooperation between different states and commercial actors has created complex surveillance networks that feed each other in ways that may be difficult to anticipate (see e.g. Lyon 2015; Mathiesen 2013; cf. Haggerty and Ericson 2000 for the “surveillant assemblage”). In recent decades, terrorism has taken on a central role in the justification of (state) surveillance (see more in e.g. Mathiesen 2013; Simone 2009), facilitating legislative changes that favour surveillance in many countries. Overall, it can be argued that surveillance in the digital age is both particularly ubiquitous and particularly elusive, a combination that gives it considerable societal power (cf. Fuchs et al. 2012; Lyon 2015).

Academic literature offers different views on how the formidable presence of surveillance in society should be evaluated. Some scholars consider surveillance solely a form of control and domination, emphasizing the fundamental power asymmetries that characterize its existence (see e.g. Fuchs 2015; Allmer 2012 for panoptic interpretations of surveillance; cf. Foucault 1977 for the panopticon). Others offer a more inclusive framework which allows for different kinds of practices, purposes and relations of power to be understood as part of surveillance, some of which might be socially beneficial and egalitarian (or at least well meant), while others not. (The latter are, however, often highlighted also among such scholars; cf. e.g. Lyon 2015; Haggerty and Ericson 2000; see more of this categorization of surveillance research in Allmer 2012). Such differences often relate to disputes about how broad an array of practices should be categorized as surveillance. While this disagreement is not central to the present paper – the type of top-down state intelligence discussed here is rarely denied the status of surveillance – the different approaches do involve different limitations for the (scope of) interpretations available about the nature of the surveillance explored here. In this paper, a strictly domination-centred view is rejected, despite clear recognition of the power asymmetries that state surveillance utilizes and creates. This is because the planning and implementation of such surveillance involves a myriad of (also democratically elected) actors, purposes and consequences, and such complexity is difficult to reduce to (an intent of) oppression. Importantly, acknowledging this does not imply disregarding the many potential risks and inevitable disadvantages associated with surveillance, such as the curtailing of privacy and related civil liberties such as freedom of expression (e.g. Lyon 2015; 2014). Rather, a recognition of the complexity of the phenomenon, and the risks inherent in it, highlights the relevance of rigorous public discussion and careful consideration before any decisions are made. For the present article, this conviction serves as motivation for the research questions and informs the interpretation of the results.

2.2. Developing Finnish intelligence legislation

Until the time of writing this article, the Finnish authorities responsible for national security have had no special mandate for data gathering. Instead, intelligence is governed by the same legislation as police work, and the use of secret methods of data acquisition is linked to particular offences and targets (Ministry of Defence 2015). This sets Finland apart from many other western countries (e.g. Sweden), where national security purposes such as the prevention of terrorism make otherwise forbidden surveillance measures available to the authorities.

In the 21st century, however, cyber security and intelligence have received increasing attention in Finnish politics. The topic was addressed in the 2010 *Society's security strategy* and the subsequent *Finnish cyber security strategy*, which recommended mapping and developing Finland's cyber security legislation. In December 2013, the Ministry of Defence established a working group to investigate Finland's present intelligence situation and formulate suggestions for improvement. The group recommended that Finland give its national security authorities access to masses of telecommunications data for national security purposes, while requiring less pre-existing information about a (potential) offence to justify a search; in other words, it recommended the commencement of broad digital surveillance measures (see section 4). The group's report, *Guidelines for developing Finnish legislation on conducting intelligence*, was published in January 2015.

In the following spring, digital intelligence was addressed in the government's strategic programme (*Ratkaisujen Suomi*). In autumn 2015, further development of the report's suggestions was divided between the Ministries of the Interior, Defence and Justice. One year later, the Justice Ministry, responsible for formulating constitutional changes, published its

proposal. The Ministries of the Interior and Defence, responsible for changes to civilian intelligence and military intelligence respectively, finished their projects in the spring of 2017. The proposals broadly followed the suggestions already made in the *Guidelines for developing Finnish legislation on conducting intelligence*, although modifications were made.

The process is still underway and further changes have since been made, for instance, to strengthen the supervision of the intelligence authorities. Although there is political will to bring the package to a vote as soon as possible, at the moment of writing this article (December 2017) the precise schedule remains open.¹

3. Critical discourse studies: political discourse and argumentation

This article draws its understanding of the relationship between language and societal phenomena from critical discourse studies (CDS; e.g. Wodak and Meyer 2016; Fairclough 1992; Pietikäinen and Mäntynen 2009). In the field of CDS, language use, also referred to as *discourse*, is considered socially constructive and thus consequential (see e.g. Wodak and Meyer 2016; Gee 2014; cf. Foucault 1972). The relationship between language use and the social world is therefore seen as dialectic (e.g. Fairclough and Fairclough 2012, 81; Pietikäinen and Mäntynen 2009). This view motivates the present article's focus on discourse and helps understand the social relevance of the way surveillance is negotiated. Furthermore, since CDS is particularly interested in the ways that discourse is connected to societal power (e.g. Wodak and Meyer 2016), it offers particularly useful insights for exploring a phenomenon like surveillance (cf. Section 2.1).

Drawing on the above view of discourse, the present article focuses specifically on political discussion. To further understand the properties particular to this type of discourse, I apply insights from Fairclough and Fairclough's (2012) work, which combines argumentation analysis and the discourse analytic framework (cf. e.g. Jokinen 1999 for argumentation analysis as a tool in discourse analysis). Based on a view of politics as *deliberation*, Fairclough and Fairclough (*ibid.*) claim that discourse associated with the field of politics should be primarily understood as argumentation. This is because deliberation is concerned with weighing and choosing between different alternatives in response to particular circumstances and goals (more on this view of deliberation below). More specifically, Fairclough and Fairclough (*ibid.*, 1, 5) believe the main types of arguments in political discourse are *practical arguments* (cf. e.g. Kakkuri-Knuuttila 1998, 86–89). They offer responses/solutions to practical problems, giving reasons for or against particular ways of acting. Therefore, such arguments also potentially ground a decision, which makes them particularly consequential (see also Jokinen 1999, 131 for the relevance of *action* in argumentation). This view fits, and therefore helps to further explore, the nature of political discussion on Finnish surveillance legislation.

Although Fairclough and Fairclough's (2012) insights play a central role in this article, some specifications and restrictions must be mentioned. Fairclough and Fairclough's (*ibid.*) work has been sharply criticized for delimiting the realm of the political to elite arenas, and for overlooking non-deliberative political situations (Hay 2013; see reply in Fairclough and Fairclough 2013). Although such criticism poses important questions about the broader theoretical implications of the approach, it presents no obstacle to applying relevant insights to the present data. This is because the data constitutes a clear example of the kind of traditionally political and deliberative discourse that this approach privileges: it includes documents which have been drafted for explicitly political purposes, in a process that has involved an array of participants with differing viewpoints, at least some of which become the topic of additional consideration (cf. Fairclough and Fairclough 2012, 11-15; more in Section 6 on analysis). It

should be emphasized that the use of the concept of deliberation here is descriptive (*ibid.*), reserved for situations which minimally involve the consideration of one counter-argument to the proposed line of action. Therefore, deliberation is treated as an argumentative genre (Fairclough and Fairclough 2012, 13) guiding the selection of analytical tools rather than as a normative ideal. A political process may constitute deliberation without being particularly “good”, balanced or democratic (*ibid.*, 14, 26–27) and, consequently, the present application of Fairclough and Fairclough’s analytical framework is in itself no comment on the (normative) deliberative quality of the data being analysed (here, Fairclough and Fairclough’s understanding of deliberation of course differs from e.g. normative models of deliberative democracy, and it has also been directly criticized by Hay 2013; however, for the current analysis it presents a useful starting point).

Lastly, it needs to be emphasized that the present article only shares some of Fairclough and Fairclough’s (2012) analytic goals and therefore its application of the framework is highly selective: besides conducting descriptive argumentation analysis (more below), Fairclough and Fairclough (*ibid.*, 51–68) draw on informal logic, (especially pragma-) dialectics and rhetoric, to formulate a strictly non-relativistic normative basis for *evaluating* both deliberative processes and the contents (rationality) of arguments (see Hay 2013, 326, and Finlayson 2013 for critique). The present article does not attempt to conduct such evaluation but instead, in alignment with more traditional discourse analytic goals (cf. e.g. Finlayson 2013, 316; Fairclough 1992; Wodak and Meyer 2016; see also e.g. Jokinen 1999 for related strands in rhetoric), focuses on showing how particular meanings are drawn upon and others excluded from debate (though see Fairclough and Fairclough 2013, 340–341 for how such questions also connect to their framework).

4. Data

This article analyses the working group report *Guidelines for developing Finnish legislation on conducting intelligence*, which can be considered a key stage in the Finnish legislative process (see section 2.2). The main, 81-page, report begins by describing the changing security environment and current state of Finnish intelligence activities as well as their legal framework, then discusses the relevant legislation in five other (western European) countries and examines domestic and international legal constraints on intelligence legislation. The report subsequently recommends several significant changes in Finnish intelligence capabilities: creating a legal basis for *foreign systems intelligence*, *foreign human intelligence* and *cross-border telecommunications intelligence*, as well as – an essential prerequisite – restricting for national security purposes the constitutional right to privacy of correspondence. The present article is primarily concerned with the recommendation concerning telecommunications intelligence, which involves the digital surveillance (interception and processing) of telecommunications that cross the Finnish border (though in practice all kinds of domestic information may be caught since data traffic has little regard for national borders, cf. cloud servers based abroad).

For telecommunications intelligence, the working group report suggests a model whereby telecommunications data would be filtered in several stages. Step by step, the number of messages searched would decrease and the pervasiveness of the investigation increase. First, all data going through selected telecommunications channels would be screened with pre-defined search criteria. In this phase, masses of citizen’s messages would be subject to search. The report suggests that, at this point, the search could mostly target identification data only (as opposed to content). It is also suggested that the screening be performed automatically to alleviate privacy concerns. After this initial screening, any data not matching the search terms

would be deleted. The remaining messages would be further subjected to manual processing, at which point also content could be examined.

The main report is followed by five appendices, two of which are selected for analysis here: a summary of commentaries from stakeholder and expert hearings (henceforth referred to as *summary*), and an opposing opinion by representatives from the Ministry of Traffic and Communications (henceforth *opposing opinion*). Together, these appendices raise a range of typical concerns about the proposed telecommunications intelligence. The summary brings together (both critical and supportive) commentaries from a wide range of organizations and people consulted during the process, representing a variety of societal roles from universities and NGOs to business and the police (cf. Section 2.1. for the multitude of actors involved in surveillance processes). Since this group involves institutions and actors playing a key role in (also other) public surveillance discussions in Finland, the appendix can be seen to illuminate not only this particular political process but also more generally the national surveillance dialogue. In the summary, the stakeholder commentaries have been paraphrased and reorganized, so the representation of these perspectives in the document itself is an interesting part of the overall negotiation over surveillance (note, too, that only particular, written commentaries originating from the participants themselves would have been accessible online, and therefore the summary provides the only available window into much of the stakeholder discussion). The sources of particular comments are not specified in the summary beyond the original list of participants. In contrast, the opposing opinion entails a comprehensive and consistent criticism of the argument for digital surveillance, (presumably) written by the sources of the criticism themselves. The authors criticize the working group for concentrating solely on finding justifications for digital surveillance and largely disregarding contrary perspectives.

The official report is publicly available, written in Finnish with summaries also in Swedish and English. This analysis uses the Finnish version; the excerpts in Section 6 have been translated by the author, although an unofficial English translation (March 2015) has assisted in this work. Special care has been taken to translate faithfully expressions central to the argumentation.

5. Analytical process

The methodological approach of this article draws on insights from the fields of CDS and argumentation analysis, especially Fairclough and Fairclough's (2012) analytical tools for the structure of argumentation. The latter, which develops insights from Walton (2006; 2007) and Audi (2006) and is particularly designed for political language, is especially useful for constructing an overview of the surveillance argument and its critique.

The main analytical concept applied in this article is *argument*, understood as a complex speech act in which a claim is justified or contested (Fairclough and Fairclough 2012, 35–38; cf. e.g. Kakkuri-Knuuttila 2004, 63; Jokinen 1999, 127; Toulmin 2003, 12). An argument involves a set of statements which entail a conclusion (*claim*) and *premises* (Fairclough and Fairclough 2012.). A claim states what kind of action ought to be taken (ibid., 45), whereas premises give reasons for that claim. Premises can be divided into four types. *Goal premises* constitute a future state of affairs that is seen as preferable to the present (e.g. ibid., 43, 45). *Circumstantial premises* describe the context of action, often described as a problem in need of solution (which is, then, the recommended action/claim; ibid., 44). Goals and circumstantial premises are informed by the *value premise* of the argument (ibid.). *The means-goal premise*, which is often presupposed, presents the usefulness of the action proposed in the claim for reaching the desired goal (e.g. ibid., 45; cf. Toulmin 2003 for *warrant*). In the deliberative process, all these parts of the argument, as well as the argument itself, may be questioned and alternatives provided. For

the purposes of this article, this analytical approach sheds light on the various types of justifications that can simultaneously be used when arguing for surveillance and the ways in which different points in the critique relate to the argument.

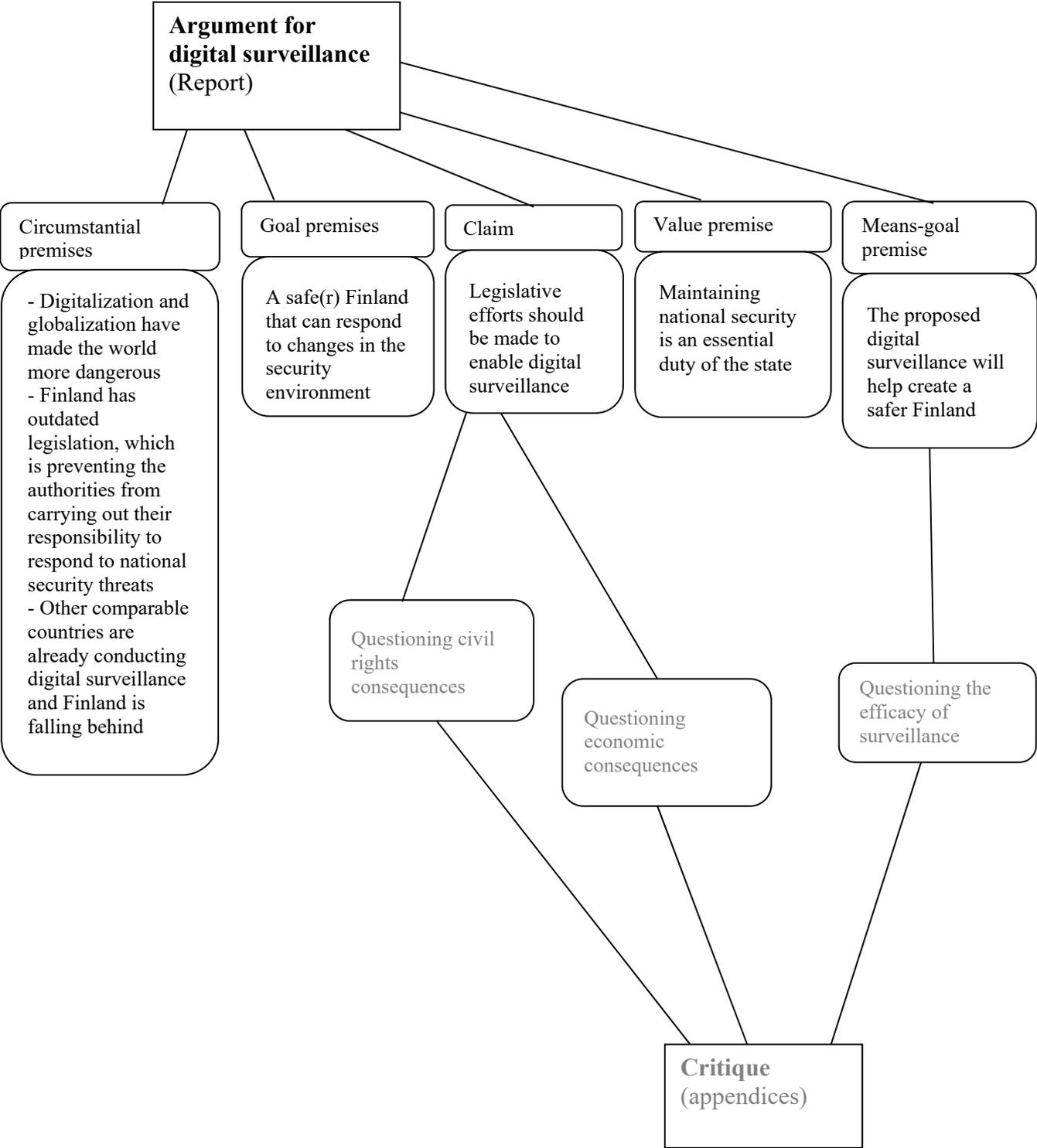
I started the analysis by mapping the working group report for statements that justified cross-border telecommunications intelligence and which thus together constructed the argument for digital surveillance. After identifying the main claim, I explored the argument's premises (see Fairclough and Fairclough 2012; Kakkuri-Knuuttila 1998, 24, 60, 101–102). It quickly became evident that isolating the justifications for digital surveillance from those for other recommendations was difficult: overall, the report makes three main arguments concerning different types of intelligence (foreign human intelligence, foreign systems intelligence and cross-border telecommunications intelligence), which are often discussed as a package. This means that they share premises and sometimes even (upper category) claims (cf. interrelationships between arguments in Kakkuri-Knuuttila 1998, 101). To keep the focus on digital surveillance, I examined all the shared elements but disregarded anything that clearly related only to other legislative recommendations, on the grounds that digital surveillance is the most controversial of the arguments and therefore much general justification can be considered relevant for it.

After reconstructing the argument for digital surveillance, I mapped the appendices for statements that were critical of any part of it, either by simply questioning it or by providing alternative accounts (see Fairclough and Fairclough 2012, 50–51). As many of the points made drew on related beliefs and formed networks of mutually supportive statements, I further classified them into thematically related strands. Three of these were selected for discussion here based on their prominence in the data and connections to societal and academic discussion on surveillance. After this, loosely drawing on Fairclough and Fairclough's (2012) examination of counter-argumentation in political discourse (e.g. debate on tuition fees, pp. 200–234; also see Fairclough and Fairclough 2013, 340–341 on “evaluation by participants” and asked and unasked critical questions), I looked at the report (and in part the summary, see Section 4) to see whether or not this critique was included in the group's consideration of surveillance, and if so, how it was presented and further addressed to alleviate the concerns expressed (see Jokinen 1999, 128–129 for the benefits of examining reception and negotiation in argumentation analysis; cf. Pietikäinen and Mäntynen 2009, and Fairclough 1992 for the relevance of choices and exclusion in discourse analysis).

6. Arguing for and against digital surveillance

This section discusses the results of the analysis. I will first present a simplified reconstruction of the argument for digital surveillance as it appears in the working group report, as well as the selected strands of critique from the appendices, in Figure 1. After the reconstruction, the argument is elaborated on with excerpts from the text. As the justifications for the argument follow the same logic throughout the report and also broadly follow an established line of surveillance legitimation found in previous studies (more below), the presentation of this part of the analysis is kept concise. To give one more detailed example of the argument's construction, the subsequent sub-section is dedicated to one particularly interesting premise, that is, the *means-goal*. This has been chosen for further elaboration because it also relates to a central strand of critique, the evocations and negotiation of which are consequently discussed. After this, the construction and negotiation of two further critique strands from the appendices, namely economic and civil rights concerns, are explored.

Figure 1. Digital surveillance: argument and critique



6.1. The argument for digital surveillance

In the working group report, the argument for digital surveillance can be said to consist of one main *claim*, indicating the desired course of action, and several supplementary, more specific, related claims. The main claim is that certain forms of digital surveillance should be legalized. The supplementary claims explain how to do this, suggesting, for example, automated screening for the initial round of data gathering. In the report such recommendations appear especially in Section 6.1.4, on *Executing telecommunications intelligence*; in this article, they have been outlined in Section 4, where the suggested model for telecommunications intelligence was introduced.

The main justification for the claim(s) lies in an extensively discussed *circumstantial premise* describing changes in Finland's security environment. This premise constructs the digital age as uniquely dangerous for national security: unprecedented threats result from both the use by dangerous individuals and groups of new communications technologies and from the potential use of technology as a weapon in cyber-attacks (cf. Steiger et al. 2017 for "cyber angst" in German discourse). Excerpt 1 from Section 1.1 (*Background*) shows one aspect of this premise:

- (1) The rapid development of telecommunications technology has made cross-border communication and networking between parties that constitute a threat to Finland faster and simpler and fuelled the internationalization of threats.

Typically of the report, technological development is here depicted solely through its potential for hostile activity. The acuteness of the threat therefore constitutes the problem that the practical argumentation attempts to solve in this document (cf. Fairclough and Fairclough 2012, 44). This depiction of the problem is complemented with descriptions of current intelligence legislation in Finland and elsewhere: the Finnish legislation is constructed as obsolete and consequently inadequate for addressing the threats of the global and digital era, while elsewhere legislation is in place that allows digital surveillance (Section 4: *International comparison*). The countries mentioned are all European democracies (e.g. Sweden, Norway), and are in fact referred to in the text as "comparable", so such descriptions alone cast doubt on Finland's current legislation. In addition to the discrepancy implied through contrast, the report also explicitly gives other countries' practices as reason for change in Finland.

Since the need for digital surveillance arises from security concerns, the *goal* of the argument is improving Finland's ability to respond to perceived contemporary threats (cf. Excerpt 1). The ultimate desired state of affairs (Fairclough and Fairclough 2012, 43) is a safer country. This rationale relates the justifications for Finnish surveillance to often examined (state) surveillance legitimation both in governmental discourse (e.g. Simone 2009) and media discussions (e.g. Wahl-Jorgensen et al. 2017; Barnard-Wills 2011), even though the specific formulation of the threat varies (for instance terrorism may play a more visible role elsewhere; e.g. Lischka 2017; cf. Tiainen 2017 for Finnish discussion). The following excerpt (Section 1.2: *Object of study*) explicates the goal premise in the report:

- (2) "The aim is to improve the ability of senior members of the government and the security authorities to obtain information on [serious national security] threats and on developments in Finland's security environment. We must be able to provide senior members of the government with timely, impartial and reliable information as input for decision-making [...]."

It should be noted that this goal is shared by all three main arguments concerning different types of intelligence in the report (see Section 5), as is the *value premise* on which this goal is based (Fairclough and Fairclough 2012, 45). This premise highlights national security as a priority. As Fairclough and Fairclough (ibid.) suggest, the value premise tends to be expressed implicitly; here it is mostly indicated by the continual focus on security and the relative absence

of discussion of other possible societal values or goals (more below). The next excerpt from Section 2.2 (*National security environment*) exemplifies this exceptionally clearly:

- (3) “Protecting the country’s sovereignty can be considered the nation’s most important concern. [...] Other key interests include directing the government, international affairs, the national defence capability, internal security, economic life and the infrastructure, and citizens’ income security and their ability to go about their daily lives. Threats against any of the above may be considered threats to national security.”

As this passage formulates a country’s core interests, it can be seen to set the value base that underlies all other, more practical considerations in the report. National security is related to every key aspect characterizing a sovereign country and is thus by definition a priority. Possible contradictory interests are not mentioned (see Section 6.4 on civil rights issues).

6.2. Constructing, questioning and negotiating the means-goal premise

The means-goal premise asserts that digital surveillance is the right way to solve the problem constructed in the circumstantial premises, and will help bring about the preferred future situation (goal). In explicit formulations of the premise, the suggested telecommunications measures are said, for instance, to “ensure”, “enable” or be “a condition for” obtaining information vital for national security. Further confirmation of the premise is sought from other countries’ surveillance practices, whose existence is constructed as validation of their usefulness (though no specific positive experiences with surveillance are mentioned). Appeal is also briefly made to international expertise, in Section 6.1.7 (*Telecommunications intelligence impact assessment*), where unidentified “foreign experts” are briefly cited, stressing the usefulness of telecommunications intelligence (cf. van Leeuwen 2007, for “appealing to authority”).

Further explication of the means-goal premise remains, however, scarce: the report mostly concentrates on describing the increasing importance and volume of digital information (thus setting the circumstantial premise), but largely presupposes that access to this vast pool of data will guarantee finding the *relevant* bits of information from it. This is important, since the omission concerns a major, both academically and publicly discussed criticism of digital surveillance (see e.g. Scheinin 2015; van Van Gulijk et al. 2014; more below). In particularly subtle evocations of such a presupposition, the relevance of the acquired information is even embedded in the definition of surveillance itself, as in the following passage:

- (4) Early-phase data acquisition will improve Finland’s prospects of preparing for threats and will broaden the range of means available to it to prevent threats being realized. (Section 5.5: *Relationship between the duties and the powers of the security authorities.*)

Early-phase data acquisition can here be seen to denote the proposed intelligence measures. The expression *early-phase* implies that the data gathered necessarily relate to some entity or event that will take place later; the remainder of the sentence explains that this refers to (national security) threats. Obtaining this relevant information, elsewhere defined as the goal of the argument (see Excerpt 2), therefore stands for surveillance itself in this passage. Such a formulation veils any possibility of failing to reach that goal and creates a situation where proving the means-goal premise is no longer about justifying the usefulness of surveillance but about proving the benefits of early-phase information gathering. The latter is arguably an easier task, since the relevance of the information is assumed, and the alternative appears to be gathering information “late”. Overall, the conflation of surveillance and its goal could be seen as a way of excluding questions of usefulness from the debate.

In both appendices, the means-goal premise is questioned from several perspectives. For instance, in the summary, the effectiveness of surveillance in combating cyber threats is unfavourably contrasted with measures that would promote the development of safer software. A straightforward example of this critique is expressed in Section 5.7 (*Mass surveillance*), where the connection between the argument's claim and (one) goal (the prevention of cyber threats) is bluntly denied:

- (5) According to the experts who were heard, the mass collection of information does not in fact help prevent cyber threats, but is a reactive practice [...].

Further critique of the means-goal premise can be found in the opposing opinion, which dedicates its third section to this. The core rationale of this critique is summarized in the title, *The efficacy of net surveillance has not been demonstrated, and alternatives have not been evaluated*. This statement criticizes both the means-goal premise itself and the deliberative process for insufficient exploration of other (less controversial) options. Such criticism is taken further by introducing *alternative circumstantial premises* that compromise the means-goal premise, namely, developments in future internet usage such as increases in data traffic and encryption which, it is suspected, will reduce the usefulness and increase the cost of digital surveillance.

The means-goal critique is addressed briefly and selectively in the report. Any overall failure to elaborate on the relationship between the argument's claim and its goal remains unacknowledged and therefore unanswered. However, the above-mentioned alternative circumstantial premises are addressed. In Section 6.1.7 of the report, encryption is described as irrelevant for gathering useful identification data and detecting cyber-attacks. As for increases in data traffic, it is claimed that sufficient additional resources and a process of selection will address any possible issues. The answers are cursory and selective, though; for instance, neither the availability of possible additional resources nor the possibility of encrypting identification data is discussed. This is also noted in the opposing opinion. Overall, then, the report addresses particular concerns relating to the means-goal premise, but the brief responses do not answer all aspects of the critique.

Summing up, the report tends to presuppose the usefulness of digital surveillance, largely relying on the implication that increasing digital information warrants increasing digital surveillance. Relevant criticism is addressed selectively.

6.3. Questioning and negotiating economic consequences

Another central strand of the critique, appearing in both appendices, questions the overall benefit of digital surveillance by speculating that it could adversely affect the competitiveness of the Finnish economy. The argument is thereby contested by reference to negative consequences which might compromise another central goal, economic growth. In Fairclough and Fairclough's (2012) view, this type of critique is especially powerful because it contests the claim of the argument, suggesting that the proposed action itself is not desirable (as opposed to just challenging particular justifications for it; cf. Kakkuri-Knuuttila 2004, 159–160). As (related) alternative premises are also evoked, this critique additionally addresses other parts of the argument.

The feared economic repercussions cover a broad array of inter-related effects, ranging from general damage to Finland's reputation to losses in client trust that would harm especially information security firms. Excerpt 6 from the opposing opinion offers one example:

- (6) “The situation that member states of the European Union spy on each other’s citizens’ and companies’ information can be considered a hindrance to the formation of the digital single market that Finland considers important.” (p. 113)

This excerpt implies that the proposed intelligence legislation will contribute to a “situation” where inter-European trust is lost, putting the *alternative goal* of the digital single market at risk. In addition to such warnings about what may be lost, the critique on the grounds of economic consequences is also conveyed by appraisals of the alternative goals that could be reached. Such statements tend to insist (converging with civil rights questions, below) that, instead of compromising people’s privacy with digital surveillance, Finland could turn its lack of surveillance into an economic advantage. Excerpt 7 from the summary exemplifies the construction of such a goal:

- (7) “By acting justly and defending the rights and independence of individuals and companies, Finland can establish itself as an intelligent digital society and the world’s leading centre of safe technology and entrepreneurship” (Section 5.4, *Finland as a safe haven of information*).

Here, “acting justly” and “defending the rights and independence of individuals and companies” stands for *not* proceeding with the new legislation, therefore challenging the ethical basis of the argument and evoking an *alternative value premise* (more in Section 6.4. on civil rights). This is followed by an alternative goal (becoming a centre of safe technology and entrepreneurship) that fits this premise, characterized by the positive expressions “intelligent” and “world’s leading”. In both appendices, the benefits of such a goal are supported with *alternative circumstantial premises* that highlight consumers’ increasing awareness of privacy and the economic potential of digitalization.

Of all the critical strands, the economic one is most explicitly and thoroughly addressed in the working group report. Most of this response occurs in Section 6.1.7, which gives several reasons (constituting circumstantial premises) for not being concerned. These highlight the positive and downplay the negative economic potential of the new legislation. The former involves better protection against cyber-attacks as well as the investor-friendly predictability of legislation, whereas the latter relies largely on summarizing a study (included as an appendix, commissioned from Gearshift Group Ltd.) that finds no negative economic repercussions in neighbouring Sweden after the legalization of digital surveillance there. It must be noted, however, that reliance on this study is sharply criticized in the opposing opinion (p. 121), which states that the study’s timeline makes it unsuitable for comparison (it excludes the post-Snowden years, when privacy breaches have received international attention) and blames the report for omitting recent opposite experiences of US firms. These criticisms remain unanswered (cf. Kakkuri-Knuutila 1998, 164 for the questionable credibility of references to expert authority when comparable, contrary opinions exist). As will be shown below, this exclusion follows a pattern in which the growing international concern over internet privacy remains unacknowledged as a relevant circumstantial premise.

In conclusion, the economic critique receives detailed attention in the report and its goal (economic growth) is thus acknowledged as relevant. However, not all concerns are given attention, and those selected for response are answered in ways that allow for the further recommendation of digital surveillance.

6.4. Questioning and negotiating civil rights consequences

The argument for digital surveillance is also challenged in the appendices by reference to the threat that it poses to civil rights, most prominently privacy. Respect for these rights constitutes both the *value premise* on which this criticism is based, and the *alternative goal* that it sets for Finnish society. Since such critique is ultimately concerned with the negative consequences of the proposed surveillance measures, it can be seen to question the claim of the argument similarly to the way the economic critique does.

The civil rights critique is often less explicitly formulated than the economic one. Typically, it is evoked by constructing surveillance as antithetic to civil rights, and the current situation as a choice between one and the other. Such a view echoes both concerns relating to the risks of surveillance discussed in Section 2.1. (and in much academic literature on surveillance, e.g. Lyon 2015; Allmer 2012), and popular post-Snowden surveillance critique expressed in the media and by politicians in Finland (see e.g. Tiainen 2017 on the “discourse of threat”) and elsewhere (e.g. Steiger et al. 2017; Lischka 2017).

The core rationale of this type of criticism is presupposed, for instance, in Excerpt 7 (above), where “acting justly” and “defending the rights and independence of individuals and companies” stand as an alternative to the planned legislation. The (potential) contrast between surveillance and civil rights is also implied in both appendices in discussions about whether the proposed intelligence measures constitute “mass surveillance”. This concept has been widely applied to NSA surveillance post-Snowden and it carries Orwellian connotations that stress the anti-democratic aspects of surveillance (cf. e.g. Allmer 2012; Lyon 1994). The following passage from the summary (Section 5.7 on *Mass surveillance*) connects the concept to the proposed legislation:

- (8) There are different views about mass surveillance. It emerged in the hearings that it is also considered to be mass surveillance when data are collected using precise search criteria from any telecommunications.

Here, data acquisition with “precise search criteria” stands for the proposed surveillance measures, and the possibility of applying the concept of “mass surveillance” to such a practice is introduced (more below on *how* this idea is presented). The negative implications of such a definition are made evident later in the same section of the summary, where the discussants are paraphrased stating that “all-encompassing monitoring is not generally acceptable”. Any claim that would support surveillance practices this broad is thereby contested.

The appendices also question the report for obscuring certain characteristics of the proposed legislation which have implications for privacy. The opposing opinion points out that the working group initially used the term *net monitoring* (verkkovalvonta) to describe the planned cross-border telecommunications intelligence, but subsequently changed the term to avoid its negative connotations. Moreover, both appendices note that, for technical reasons, the proposed telecommunications intelligence will inevitably also catch domestic communication (which makes questions of privacy more pertinent). This stands in contrast to the term “cross-border”, which the opposing opinion consequently criticizes as deliberately misleading. Thus, concerns about the civil rights consequences are linked to doubts about the sincerity of the deliberative process.

Criticism of the nature of surveillance is complemented with alternative accounts of relevant *circumstantial premises* in the appendices. For instance, the opposing opinion accuses the report of unduly excluding the Snowden revelations and their aftermath from its description of the current societal situation. It is pointed out that the revelations increased societal attention to

online privacy and hardened attitudes towards surveillance, which should be taken into consideration. Here, the civil rights critique converges with the economic critique, since the concern for privacy is predicted to translate into economic repercussions.

In the report, the rationale and value base of the civil rights critique receives limited acknowledgement. Most discussion relating to civil rights appears in Section 6.1.2 (*Requirements of international human rights agreements and the Constitution*), which offers an examination of Finland's human rights commitments in the light of the suggested legislative changes. The focal content of the protected rights is described, but the report's focus is on how these rights can be legally restricted. Revealingly, Section 6.2.2.2. on *Article 8 of the European Convention of Human Rights* includes four sub-sections, all of which are exclusively concerned with the legality of infringing the protected rights (entitled e.g. *Permitted infringement of the rights guaranteed by Article 8(1) [...] and National security as an interest allowing interference*). A similar absence of recognition for any priority of such rights can be detected in Excerpt 3, where a nation's "key interests" are listed. These range from income security to infrastructure, but there is no mention of democratic freedoms. Altogether, the report presents constitutional and human rights regulations primarily as potential obstacles to be circumvented.

The thinness of the response to the civil rights critique is underlined by the report's treatment of the Snowden revelations (also noted in the opposing opinion, above), which provoked popular outrage much along the lines of this critical strand (more e.g. in Tiainen 2017). The revelations are explicitly mentioned in the report only in Section 6.1.7 where, referring to the study by Gearshift Group Ltd., it is speculated that "clear" intelligence legislation could actually give a competitive (economic) edge in the post-Snowden world. Given the widespread outrage against privacy infringements following the revelations, this constitutes remarkably selective treatment of the topic. Also the summary refers to the revelations and their aftermath only implicitly, with the expressions "the world's lack of confidence in current [business-] actors" and "recent international events". The brevity and imprecision of the expressions indicates that they are paraphrasing the original discussions, and these formulations can therefore be interpreted as part of an evasive response to the criticism related to the Snowden revelations. In short, the lack of explicit reference enables the association to be kept to a minimum and can be seen to contribute to a pattern of avoiding any broader discussion of mass surveillance and civil rights considerations in the report.

There is, however, one particular criticism which does get addressed in the report, and its discussion is worth a closer look. This criticism concerns the interception of domestic data in cross-border telecommunications intelligence (above), and a reaction can be found in Section 6.1.7:

- (9) It was brought up in the hearings that for technical reasons it is not always possible to distinguish between domestic and international telecommunications. Any infringement of the protection of the confidentiality of correspondence could therefore in theory also affect domestic telecommunications. In such cases, the protection of confidentiality could be upheld by prohibiting the processing of domestic telecommunications and requiring the immediate deletion of any such information.

It is worth noting here that the expressions "not always" and "in theory" undermine the problem presented, which was described in the appendices as unavoidable and continuous. Also the expression "brought up" signifies novelty, which for both the scope and the relevance of the problem seems unlikely and therefore strategic. The solution that is subsequently offered (last sentence) addresses the handling but not the interception of domestic data, thus limiting the scope of what constitutes confidentiality. This example has an interesting parallel to Excerpt 8, from the summary, where the idea that the term *mass surveillance* could be applicable to the

proposed intelligence is summarized in a way (with the expression “also”, followed by specifications of the proposed surveillance measures) that downplays a widely debated point of criticism. Thus both excerpts employ expressions that simultaneously convey a central point of the critique and subtly undermine its relevance and prevalence.

Overall, then, it can be stated that the report discusses civil rights implications from a very selective perspective, and the relevant critique is largely ignored or at least downplayed. Acknowledgement of the core rationale and topicality of the critique is especially avoided. The consistency of such absences excludes this line of critique from deliberation.

7. Conclusion

An examination of the working group report has revealed how the argument for digital surveillance is constructed: the present social situation is depicted as threatening and Finland as uniquely unprepared for it (*circumstantial premises*); national security is highlighted as a social priority (*value premise*); a future is envisaged where Finland is prepared for the challenges it will face (*goal premise*) and digital surveillance is presented as the right way to get from here to there (*means-goal premise*). Corresponding legislative action is called for (*claim*). Similar justifications for surveillance have been observed both in concurrent Finnish media discussion (Tiainen 2017) and in other countries where surveillance has gained further ground (cf. e.g. Steiger et al. 2017 for Germany, Tréguer 2017 for France and Hintz and Brown 2017 for Britain).

Having examined the argument itself, three strands of critique from the appendices as well as their negotiation have been explored to gain an understanding of the choices made in the deliberative process. One strand challenges the means-goal premise for being inadequately proven. Selected parts of this critique are addressed in the report, but the way that this premise tends to rely on presupposition makes its rationale elusive. Another critical strand has to do with the civil rights consequences of the argument. In the report, the concerns driving this strand are largely ignored; instead, relevant themes tend to be reduced to regulations that potentially stand in the way of the goal of the argument. A third strand concerns the economic repercussions of surveillance. Of all the strands of the critique, this one receives most attention in the report, although eventually it is found inadequate to change the conclusion of the argument. The explicit attention given to it can nevertheless be seen as an acknowledgement of the societal value and relevance of economic growth.

The above-described negotiation over surveillance sheds light on the way broadening intelligence measures are advanced (even) in a time when there is widespread indignation over surveillance (cf. e.g. Tréguer 2017 for the Snowden paradox). Although critical views are expressed, their relevance is reduced as some of the main concerns simply remain unanswered (cf. Hintz and Brown, 2017, for unequal degrees of influence granted to different stakeholders in Britain). In the present case, especially the broad exclusion of the means-goal and civil rights critique from the report is notable since these relate to widely circulating post-Snowden concerns both in Finland and abroad (e.g. Wahl-Jorgensen et al. 2017; Lyon 2015; Tiainen 2017, Scheinin 2015). The report also consistently avoids mentioning the Snowden revelations, which can be considered an attempt to distance the Finnish case from any related outrage or comparisons (see Tréguer 2017 for similarities in the French political process). Consequently, instead of participating in a discussion over possible excesses in surveillance globally, the report treats other countries' intelligence practices simply as confirmation of the lack of capabilities at home. Such straightforward dismissal of a major point of controversy confirms the persistency and strength of the national security argument.

The selective treatment of the critique also means that, although Fairclough and Fairclough's (2012) permissive criteria for what constitutes deliberation are fulfilled, the data shows little of the thorough consideration that was called for in Section 2.1., given the multifaceted view of surveillance. Such consideration was seen as particularly relevant since surveillance in this view was acknowledged to involve both a variety of motivations and consequences, as well as potential power asymmetries and risks regarding, for instance, privacy and (other) democratic freedoms. In the Finnish case, even with the extended democratic process and the multitude of actors involved, the lack of consideration of some major concerns highlights the continued prevalence of such risks.

Acknowledgments

I would like to thank Anne Mäntynen, the two anonymous reviewers as well as my colleagues at the University of Jyväskylä for useful feedback and support in the development of this article.

¹¹ At the time of revising this article (October 2018), the necessary changes to the constitution have been accepted by the parliament. The actual intelligence legislation has not yet been passed, but may now be voted on before the parliamentary elections April 2019.

References

- Audi, Robert. 2006. *Practical Reasoning and Ethical Decision*. London: Routledge.
- Allmer, Thomas. 2012. *Towards a Critical Theory of Surveillance in Informational Capitalism*. New York: Peter Lang.
- Barnard-Wills, David. 2011. "UK News Media Discourses of Surveillance." *The Sociological Quarterly* 52 (4): 548–567. doi: 10.1111/j.1533-8525.2011.01219.x
- Fairclough, Norman. 1992. *Discourse and Social Change*. Cambridge: Polity.
- Fairclough, Isabela, and Norman Fairclough. 2012. *Political Discourse Analysis: A Method for Advanced Students*. Abingdon: Routledge.
- Fairclough, Isabela, and Norman Fairclough. 2013. "Argument, Deliberation, Dialectic and the Nature of the Political: A CDA perspective." *Political Studies Review*, 11(3): 336–344. doi: 10.1111/1478-9302.12025
- Finlayson, Alan. 2013. "Critique and Political Argumentation." *Political Studies Review*, 11(3): 313–320. doi: 10.1111/1478-9302.12023
- Foucault, Michel. 1972. *The Archaeology of Knowledge*. London: Routledge.
- Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. London: Penguin Books.
- Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. 2012. "Introduction: Internet and Surveillance." In *Internet and Surveillance. The challenges of Web 2.0 and Social Media*, ed. by Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 1–30. New York: Routledge.
- Fuchs, Christian. 2015. "Surveillance and Critical Theory." *Media and Communication* 3(2): 6–9. doi: 10.17645/mac.v3i2.207
- Gee, James Paul. 2014. *An Introduction to Discourse Analysis: Theory and Method*. Abingdon: Routledge.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51(4): 605–622. doi: 10.1080/00071310020015280
- Hay, Colin. 2013. "Political Discourse Analysis: The Dangers of Methodological Absolutism." *Political Studies Review*, 11(3): 321–327. doi: 10.1111/1478-9302.12026
- Hintz, Arne, and Ian Brown. 2017. "Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden." *International Journal of Communication*, 11(20): 782–801.
- Jokinen, Arja. 1999. "Vakuuttelevan ja suostuttelevan retoriikan analysoiminen [Analysing persuading and convincing rhetoric]." In *Diskurssianalyysi liikkeessä [Discourse analysis in motion]* ed. by Jokinen, Arja, Kirsi Juhila, and Eero Suoninen, 126–159. Tampere: Vastapaino.
- Kakkuri-Knuuttila, Marja-Liisa. 1998. *Argumentti ja kritiikki. Lukemisen, keskustelun ja vakuuttamisen taidot [Argument and critique. The skills of reading, conversation and convincing]*. Helsinki: Gaudeamus.
- Kunelius, Risto, Heikki Heikkilä, Adrienne Russell, and Dmitry Yagodin (eds.). 2017. *Journalism and the NSA Revelations: Privacy, Security, and the Press*. London: IB Tauris.
- Lischka, Juliane A. 2017. "Explicit Terror Prevention Versus Vague Civil Liberty: How the UK Broadcasting News (De) Legitimatises Online Mass Surveillance Since Edward

- Snowden's Revelations." *Information, Communication & Society* 20(5): 665–682. doi: 10.1080/1369118X.2016.1211721
- Lyon, David. 1994. *Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minneapolis Press.
- Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1(2): 1–13. doi: 10.1177/2053951714541861
- Lyon, David. 2015. *Surveillance after Snowden*. Cambridge: Polity Press.
- Mathiesen, Thomas. 2013. *Towards a Surveillant Society: The Rise of Surveillance Systems in Europe*. Sheffield on Loddon: Waterside Press.
- Marx, Gary T. 2002. "What's New about the 'New Surveillance'? Classifying for Change and Continuity." *Surveillance & Society* 1(1): 9–29.
- Ministry of Defence. 2015. "Guidelines for Developing Finnish Intelligence legislation: Working Group Report", accessed December 14, 2017, https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf
- Ni Loideain, Nora. 2015. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, 3(2): 56–62.
- Pietikäinen, Sari, and Anne Mäntynen. 2009. *Kurssi kohti diskurssia [Course towards discourse]*. Tampere: Vastapaino.
- Scheinin, Martin. 2015. "The State of Our Union: Confronting the Future." *International Journal of Constitutional Law* 13(3): 559–566. doi: 10.1093/icon/mov051
- Schulze, Matthias. 2015. "Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal." *Surveillance & Society* 13(2): 197–217. doi: 10.24908/ss.v13i2.5296
- Scollon, Ron, and Suzie Wong Scollon. 2004. *Nexus Analysis: Discourse and the Emerging Internet*. London: Routledge.
- Simone, Maria A. 2009. "Give Me Liberty and Give Me Surveillance: A Case Study of the US Government's Discourse of Surveillance." *Critical Discourse Studies* 6(1): 1–14. doi: 10.1080/17405900802559977
- Steiger, Stefan, Wolf J. Schünemann, and Katharina Dimmroth. 2017. "Outrage without consequences?: Post-Snowden Discourses and Governmental Practice in Germany." *Media and Communication* 5(1): 7-16.
- Tiainen, Minna. 2017. "(De)legitimizing Electronic Surveillance: a Critical Discourse Analysis of the Finnish News Coverage of the Edward Snowden Revelations." *Critical Discourse Studies*, 14(4), 402-419. doi: 10.1080/17405904.2017.1320296
- Tréguer, Félix. 2017. "Intelligence Reform and the Snowden Paradox: The Case of France." *Media and Communication*, 5(1): 17-28.
- Toulmin, Stephen E. 2003. *The Uses of Argument*. Cambridge: Cambridge University Press.
- Wahl-Jorgensen, Karin, Lucy Bennett, and Gregory Taylor. 2017. "The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates after the Snowden Revelations." *International Journal of Communication*, 11: 740–762.
- Van Gulijk, Coen, et al. 2014. "Paper Assessing Surveillance in the Context of Preventing a Terrorist Act." *Seventh Framework Programme. Surveillance: Ethical Issues, Legal Limitations, and Efficiency*, Accessed December 14, 2017, <https://surveille.eui.eu/research/publications/>

Walton, Douglas. 2006. *Fundamentals of Critical Argumentation*. New York: Cambridge University Press.

Walton, Douglas. 2007. *Media Argumentation*. New York: Cambridge University Press.

Van Leeuwen, Theo. 2007. "Legitimation in Discourse and Communication." *Discourse & Communication* 1(1): 91-112. doi: 10.1177/1750481307071986

Wodak, Ruth, and Michael Meyer (eds.). 2016. *Methods of Critical Discourse Studies*. Los Angeles: Sage.