SJPA
26(1)

Key Stakeholders’ Frames on the Police and Intelligence Agencies’ Online Surveillance Capabilities in Finland

Anna Leppänen and Jarmo Houtsonen*

Anna Leppänen,
Police University College,
Finland;
JKK School of Management,
Tampere University, Finland
anna-riitta.leppanen@polamk.fi

Jarmo Houtsonen,
Police University College,
Finland
jarmo.houtsonen@polamk.fi

Abstract

Authorities' online surveillance powers touch the very core of democracy, human rights and privacy. Thus, the legislation and its implementation must be both sustainable and legitimate in the eyes of the citizenry. We argue that the general elements of legitimate and sustainable online surveillance system can be derived from many international sources, but the crux of the matter is to adjust the general principles into country-specific conditions through well-informed, reasoned and inclusive national legislation preparation and regular follow-up discussions.

We explored how 25 key stakeholders from various fields consider 45 statements on online surveillance at the time of preparation of the intelligence legislation in Finland in 2018. Q-factor analysis arranged the stakeholders in three factors indicating distinctive frames that we named *Balancing privacy and security*, *Protecting human rights* and *Expanding surveillance powers*. With regard to enhancing further public discussion towards the interests of stakeholders, we also detected ambiguous issues, deal-breakers and areas of consensus that can be used for finding common ground in future considerations. Our study contributes particularly to research on online surveillance policy. We also demonstrate, along with some earlier findings, that Q-methodological research can provide powerful means to feed public policy discussion in the spirit of deliberative democracy.

Keywords:
online surveillance,
online intelligence,
q-methodology,
intelligence capabilities,
policy debate

Introduction

Western democracies have granted more online surveillance powers to security authorities during recent decades (Lyon 2015; 2007; Lemieux 2019). These institutional and legal changes have also pushed policing from criminal investigation to a more ambiguous field of crime control, pre-emptive measures and risk assessment (Ericson and Haggerty 1997). At the same time, the blurring of the boundaries between foreign and domestic security has expanded the role of secret services (Bauman et al. 2014; Shiraz 2017). The improved surveillance capabilities are justified by their supporters as a necessary security-increasing response against evolving threats, especially terrorism, violent extremism, cyber-attacks and espionage (Leigh and Wegge 2019; Lemieux 2019; Sivan-Sevilla 2019).

By contrast, networked civil society has expressed concerns about the negative consequences of intelligence, such as the eroding of privacy, fundamental rights and democracy, and therefore, called for more transparency and stronger oversight of intelligence operations (Shiraz 2017; Richards 2013 p. 1936). Indeed, The European Court of Human Rights (ECtHR) has addressed, through its judgements, several conflicts between surveillance and the European

*Anna Leppänen (PhD candidate) is a researcher at the Police University College, Finland. Her research interests lie in policing cybercrime, e.g. the police’s role in the network against cyber criminals, how digital technologies are shaping police work, and how people perceive security authorities’ online surveillance capabilities.

Jarmo Houtsonen (PhD) is a Senior Researcher at Police University College of Finland. His main research interests include police governance, community policing and the policing of domestic violence. He has collaborated widely in several national and international research and development projects.

Scandinavian Journal of
Public Administration
26(1): 3 – 27
© Anna Leppänen, Jarmo
Houtsonen and School of
Public Administration 2022
ISSN: 2001-7405
e-ISSN: 2001-7413

Convention on Human Rights and tried to establish criteria for acceptable through its judgements, several conflicts between surveillance and the European Convention on Human Rights and tried to establish criteria for acceptable surveillance practices[1]. These critical reactions together with widely published Edward Snowden’s disclosures have forced the leading Western intelligence countries to take a step back and increase the level of accountability and legitimacy of online surveillance through restrictions (Sivan-Sevilla 2019).

A consensus has been reached between various stakeholders on the need of effective mechanisms for oversight, accountability and transparency of the surveillance system as well as on the requirement for interfering in privacy only when it is necessary, proportional and justified by a legitimate aim. However, there is no agreement on the details of what does this entail in practice (e.g. FRA 2017). The solution of a complex, or wicked, societal problem in a democratic society, such as the scope and control of surveillance measures, requires an extensive and rational discussion, because it cannot be framed simply as a technical problem (Rittel and Webber 1973; Head and Alford 2015; Dryzek 2000). Multiple forces, including political coalitions, national and international norms, court rulings, advocacies and campaigns, advancements in digital technology, not to mention business interests, shape the discussion on surveillance powers (Hintz and Brown 2017; Hintz and Dencik 2016). Unfortunately, public debate on intelligence capabilities is often fragmentary and dispersed on several forums, focusing on few topics at a time and driving the participants easily into fixed and antagonistic positions (Bernal 2016: 243-253). Furthermore, the media acts as a gatekeeper and sets the agenda for public discussion (Hintz and Brown 2017; Hintz and Dencik 2016: 9-10). Some authors (Wahl-Jorgensen et al. 2017; Murakami Wood and Webster 2016) argue that journalists forget too easily their role as watchdogs and tend to rely on official sources, which leads to normalizing and legitimizing state surveillance. To examine and enhance the public discussion about online surveillance policy and legislations we approach these complex issues from the perspective of deliberative democracy that underlines inclusive participation in a policy debate, a critical examination of relevant information and an equal consideration of all viable policy alternatives (Cohen 1997; Dryzek 2000; Setälä 2014).

The empirical case of our study is the preparation of the new intelligence legislation in Finland. The case is a particular manifestation of a more general, complex and current policy problem of how to organise online surveillance powers of the state intelligence agencies legitimately. Thus, we first aim to increase understanding of the recent policy debate on surveillance in Finland by answering two empirical research questions. How do the key stakeholders to policy debate frame the proposed expansion of the intelligence agency’s surveillance powers? What are the major points of dissents and consensus among the views hold by the key stakeholders? We identify the frames and the policy points by following Q-methodological procedures that prompt the carefully selected group of stakeholders to sort out publicly presented statements and arguments according to their predilections.

The second aim of our paper is to enhance the public discussion and explore whether our methodological choices could show directions towards a better-informed policy discussion in the future. More specifically, we aim to demonstrate that Q-methodological research not only produces knowledge about the viewpoints on contested policy issues, but also potentially improves the quality and comprehensiveness of policy discussion. First, following the spirit of deliberative democracy, Q-method can systematize all pertinent policy arguments in the form of explicit statements. Second, Q-interview provides the participants to the debate an opportunity to reflect the subject matter and explicate their views. Third, Q-method guides the researcher, but also the participants, to understand the complexity of the policy issue and its rootedness in multiple values and interests hold by the debaters. Finally, Q-methodological research can point out and clarify ambiguous issues, areas of consensus and deal-breakers. We suggest that a similar research design is applicable in other domains of public policy debate too. Q-design would be useful in particular when public debate has a genuine opportunity to shape the outcome, for example, during an early phase of legislation drafting process or as a follow-up measure for ensuring that a conflicted decision is scrutinized with new evidence. We regard that Q-methodology in policy research aligns readily with deliberate democracy, an ideal model for reasoned, inclusive and transparent policy discussion seeking for an acceptable decision instead of the rule of the strongest and loudest (Dryzek 2000; Setälä 2014; van Eeten 2001b). These principles of deliberative democracy and Q-methodology should be valued and actively promoted as counterforces of populism, polarization or inability to reciprocate in discussion that are unsustainable but gaining ground in democratic societies (Bächtiger et al. 2018).

Towards an Acceptable Policy Through Deliberation

In this paper, we investigate within the framework of deliberative democracy, online surveillance policy debate, which took place before the Finnish Parliament decision on intelligence legislation. Deliberative democracy is a paradigm or normative ideal for socio-political decision-making that goes beyond elite's struggles for power and influence with an emphasis of reason-giving through discussion instead of majority rule. It developed gradually between 1980 and early 1990s from various theoretical approaches but has early philosophical roots much further (Floridia 2018; Chambers 2018). For example, Jürgen Habermas' communicative theory (1984) and John Rawls theory of political liberalism (1996), both on their own, significantly contributed to the theoretical and conceptual fountains of deliberative democracy, although, also many other theorists have influenced in its development, orientations or contemporary understandings (Floridia 2018).

There is no unanimous conception of deliberative democracy, but at its broadest, it can be "any practice of democracy that gives deliberation a central place" (Bächtiger et al. 2018, 2). Furthermore, there are many ideals and core features, which are typically linked to deliberative democracy. For example, mutual respect, wide participation, gradual preference formation when solving complex policy problems and aiming at consensus as well as clarifying conflict are all mentioned as essential features of deliberative democracy (Bächtiger et al. 2018). Consequently, inclusive and reasoned discussion presupposes the exploration of all relevant information, arguments and alternatives. Aiming at the common good rather than some narrow self-interests renders subsequent policy decisions more acceptable and legitimate by most people. Compromises and concessions may have to be made and the final solution may not be totally congruent with everyone's values and preferences. (E.g., Cohen 1997; Dryzek 2000; Setälä 2014.) In democratic societies, deliberation should be an encouraged ambition, because it helps citizens and stakeholders to become aware of their own and other parties' frames or values they are unwilling to trade or compromise. In other words, if a disagreement is not solvable through discussion, people at least understand the issues behind the result of the vote (Bächtiger et al. 2018; Gutmann & Thompson 2004). Furthermore, decisions must also be reviewed retrospectively and remember that they are not perennial, but for example, legislation needs amending time to time (Gutmann & Thompson 2004).

Direct citizen involvement is sometimes described as an ideal form of deliberative democracy but is often found to be difficult in practice. An access to information and presenting it in understandable form are premises of deliberative justification, but in general, complexity of problem tends to decrease citizenry's direct participation (Rosenberg 2014; Gutmann & Thompson 2004). Indeed, the details of surveillance legislation or technological means are not easy to understand even by an enlightened citizens[2] or political representatives. Consequently, surveillance is a policy issue that resists the participation of all but the most well-informed citizens. Furthermore, information is unevenly distributed among the debaters, since details of national security are disclosed only to rare. However, relying on experts is not necessarily a problem, if experts are trustworthy in the eyes of citizens, validate their views and are not afraid of challenging each other's opinions (Gutmann & Thompson 2004). Yet, to avoid the domination by a "surveillance elite" (cf. Kreissl and Wright 2015: 362) stakeholders have a responsibility to function as credible brokers between the policymakers, interest groups and citizens.

Debating and Drafting Intelligence Legislation in Finland

The tradition of political decision-making in Finland share some features that are associated with deliberative democracy. The multiparty political system in Finland presupposes coalition governments and readiness to compromise and make concessions in order to reach political decisions. However, party discipline is strict and majority governments work according to carefully drafted governmental programmes. Interest groups have institutionalised their role in pre-parliamentary policy preparation—a form of traditional Nordic model called routine corporatism (Vesa, Kantola and Binderkrantz 2018; Arter 2006). Rather than lobbying the MPs directly, Finnish interest groups prefer direct contact with the public servants and ministers, and seek for membership in various working groups and committees (Vesa, Kantola and Binderkrantz 2018: 250-252). Such conditions for policymaking and legislation highlight the importance of a thorough preparatory phase, the wide hearings of experts and the statements from stakeholders, before the actual debate in Parliament. In other words, that is the phase where the main deliberation occurs and where the stakeholder inclusion is encouraged. The preparation of the Finnish intelligence legislation followed the tradition of Nordic routine corporatism involving an inclusive and intensive stakeholder dialogue and an effort to reconcile between various interests (Kortesoja, Kunelius and Heikkilä 2019).

In 2013, the Ministry of Foreign Affairs of Finland was revealed to have been suffering from a state-sourced, undetected cyber espionage for years[3]. In this context, the authorities in charge of national security regarded Finland's status as a state without powers to gather intelligence on the threats of national security unbearable. A working group of governmental officials was appointed by the Chief Secretary of the Ministry of Defence to draft the guidelines for developing Finnish legislation on intelligence. (Puolustusministeriö 2015.) The policy debate around intelligence legislation focused especially on one proposed capability, a signals intelligence technique referred to as network traffic intelligence, which would gather information from telecommunications cables crossing the Finnish border (Puolustusministeriö 2015). The globally recognised problem is whether gathering intelligence on fibre optic cables can be sufficiently targeted, or is it some type of mass surveillance (Bernal 2016: 248; Murray and Fussey 2019: 34-36)?

The Finnish debate quickly turned into a dispute and the working group ended up handing over a discordant final report about the guidelines for legislation on intelligence (Puolustusministeriö 2015). For instance, the Ministry of Communications and Transport recommended that Finland should abstain from legislating on network traffic intelligence, questioned its effectiveness and highlighted the possible harm to the competitiveness of businesses (Liikenne- ja viestintäministeriö 2014). According to Tiainen (2019) the working group and its final report failed to respond and address adequately to the concerns of some stakeholders. The misgivings raised in Finland about the possibly detrimental effects of surveillance on civil rights, doubts about the efficacy of online surveillance methods, and the calls for transparency and effective oversight of intelligence systems are typical of the public debate in other countries too (Bernal 2016; Cayford and Pieters 2018; Murray and Fussey 2019; Omand and Phythian 2013; RUSI 2015).

The difficulties to reach consensus during the first phase of the Finnish debate on intelligence legislation can be understood through framing theory that has been successfully applied to the analyses of policy debates elsewhere (van Hulst and Yanow 2016; Rein and Schön 1996; Schön and Rein 1994). The theory postulates that the participants to the policy debate hold different frames rooted in deeply held value perspectives. These frames induce participants being selective in their consideration of different information and arguments relating to policy problems. For instance, in the context of public debate about online surveillance complex issues are often framed simple as an opposition between the individual right to privacy and the collective right to security (Bernal 2016; Lyon 2007: 176). Indeed, during the early debate on the intelligence laws in Finland, Sirkkunen and Haara (2017) detected two critical viewpoints that framed the proposed network traffic intelligence as a threat to fundamental rights and business opportunities based on privacy protection. The third viewpoint framed the legislation essentially as an opportunity to support national security and argued for new intelligence capabilities.

As a response to the critique for the proposed surveillance capabilities, the legislative preparation continued in a more inclusive manner. A follow-up group representing all parliamentary parties was established. Furthermore, a business sector representative was named in the new preparatory working group, indicating government's efforts to establish rapports with the surveillance industry and the service providers for online communication (Bernal 2016: 260; Kreissl and Wright 2015, 362-363).

The second phase of the intelligence legislation preparation resulted in a package of new laws. Act on the Oversight of Intelligence Gathering (121/2019), Act on the Use of Network Traffic Intelligence in Civilian Intelligence (582/2019), Act on the Military Intelligence (590/2019), and an amendment to the Police Act (581/2019) came fully into effect in 2019. The existing crime-based surveillance capabilities were expanded to cover also so-called serious threats to national security, and a couple of new intelligence measures was introduced. Security Intelligence Service and the Defense Forces may both operate abroad too, and have access to network traffic intelligence, where cross-border network traffic in the predefined parts of the public network is filtered against search criteria and analyzed. The oversight mechanisms were strengthened. First, an Intelligence Ombudsman was introduced to supervise intelligence and the realization of fundamental rights. Second, parliamentary oversight was strengthened in the form of Intelligence Oversight Committee. Finally, the use of most surveillance measures requires an independent judicial authorization process.

The Q-Methodological Research Design

Q-methodological research potentially can help clarifying complex political issues by disclosing the latent frames underneath the views of participants in the political debate (Dryzek and Holmes 2002; Pirkkala 2017). It can explicate the finer areas of consensus and dissent, but also ambiguous issues. Moreover, Q-methodology can detect previously unrecognised points of agreement that are conducive to further discussion and reaching an acceptable decision (Clarke 2007; Ellis, Barry and Robinson 2007; van Eeten 2001a; Durning and Brown 2006). In other words, Q-methodology can be utilised as a systematic method to structure policy issues, and therefore, support moving from a frame-critical policy analysis to a "frame-reflective policy practice" during which views can also be revised (cf. Rein and Schön 1996; Schön and Rein 1994; Pirkkala 2017). The foregoing qualities of Q-methodology make it a usable tool for improving policy deliberation and debate. Indeed, the compatibility between Q-methodology and deliberation has been demonstrated in previous case studies (e.g. van Eeten 2001a and b; Pirkkala 2017).

Data Collection

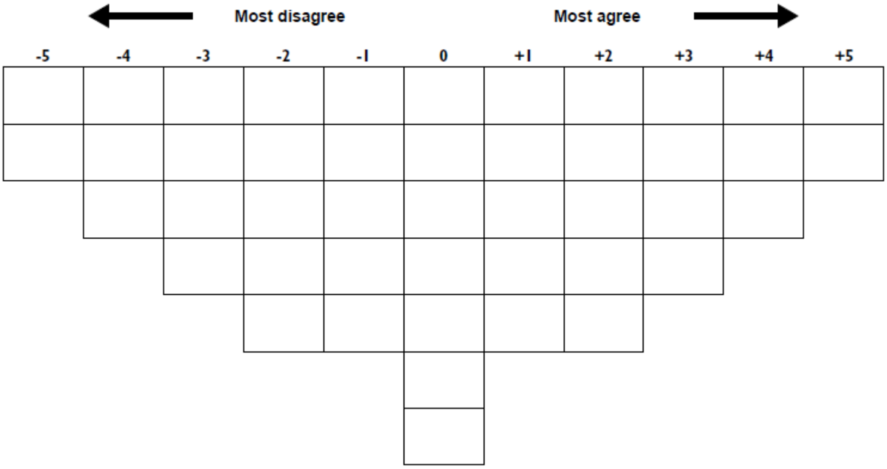
We followed the established Q-methodological research protocol in our study. First, we identified the so-called "concourse", or the trait universe covering all the relevant items belonging to the topic of research (Stephenson, 1950, 1978 as cited in Brown 1980: 186; Durning and Brown 2006: 540; Dryzek and Holmes 2002: 24). In our study, the items consisted of statements, opinions and arguments presented in Finnish policy documents, stakeholder commentaries, newspapers or social media sources about online surveillance and the proposed legislation and intelligence agencies' capabilities to conduct online surveillance. We focused mostly on the recent debate after publication of the Intelligence Law proposal drafts in spring 2017 (Sisäministeriö, 2017; Puolustusministeriö, 2017; Oikeusministeriö, 2017), which launched the second phase of the debate.

In total, we were able to detect over 700 relevant statements, which were entered into NVivo qualitative analysis software and classified to 11 broad themes. Since the data collection was part of an international project, the research instrument was designed together with Norwegian and Scottish research teams. Around 60 of the most salient statements representing the main aspects of the discussion were selected, translated into English and compared with the statements collected in Norway and the UK. After several workshops, comments and a pilot study in each country we confirmed a sufficient overlap of the most important items in each country (see, e.g. Lehtonen and Aalto 2016). Then, the final set of 45 statements was created and translated back into Finnish and printed on laminated cards. The coverage of the selected 45 statements with regard to the original 700+ statements was reviewed by re-thematising the statements back to the 11 themes and was deemed acceptable.

For this article we analysed 25 face-to-face Q-sort interviews conducted in Finland between June and September 2018. The data collection took place after the intelligence law proposals had been revised based on stakeholder comments and submitted to the Parliament as Government bills, but before the Parliament had considered them. Prior the interview, participants got an information sheet about the study, were given an opportunity to ask more details about it and signed an informed consent before the data collection began. Each interview session produced background information of the participants, a saved ranking of the statement cards and a recorded post-sort interview, during which the participants explained their choice of rankings. A typical interview lasted 1.5 hours as a whole, while the recorded and transcribed post-sort interviews were between 19 and 76 minutes. In total, we had about 20 hours of recorded material.

In the beginning of the card-sorting exercise, informants were instructed to familiarise themselves with the 45 cards, each including one statement. Then, they were asked to arrange cards into three piles: agree, disagree and neutral. The neutral pile was for cards that raised mixed feelings or were otherwise difficult to assess. The next task was to refine the division by selecting two statements from the "agree" pile that the interviewee agreed with the most and place them onto the grid (Figure 1) under the value +5. After that, respondents selected the next three statements they agreed with the most (value +4) among the statements remaining on the "agree" pile. The sorting proceeded until all statements placed into the "agree" pile were arranged onto the grid. Then, the same procedure from the extreme to milder views was followed with the statements sorted into the "disagree" pile. Finally, participants sorted the pile of "neutral" statements. The grid has 45 boxes, one for each card, and respondents could switch the places of statements as many times as they wished. After the respondents had completed the sorting exercise, the researcher saved the ranking and asked the respondents to reflect the ranking aloud on to the tape. To ensure adequate coverage of the statements, we asked at the end of the interview whether the respondents felt that some statements were missing.

Figure 1. The Fixed grid for placing the statements



We identified the names and organisations of the potential participants during the mapping of policy debate by searching for statements about online surveillance. The purpose was to find knowledgeable participants covering so that all salient stakeholders and viewpoints were covered (Brown 1980: 194; Watts and Stenner 2005). Potential participants were grouped into eight categories: Active citizens, Business, Media, Oversight organisations, Politicians, Public authorities, Researchers and Others for other relevant individuals. Within each category, we tried to select as diverse group of participants as possible. For example, researchers represented fields of study, politicians came from several political parties and NGOs were concerned with both online and offline rights. Only a few candidates turned down our invitation, but on an analysis of publicly voiced opinions by representatives of missed organisations, we still regard the coverage as being very good.

We had seven female and 18 male participants of whom almost all had at least a master's level degree. The most typical fields of study were law (10 respondents), technology (7) and social/political science (7). Several participants held more than one degree. Six respondents were 39 years of age or younger, nine were between 40 and 49, and ten were 50 years old or more. The data were anonymised and only a limited amount of background information was saved in order to guarantee respondents' anonymity. Therefore, the categories describing participants were reduced to only four: Interest group, User, Politician and Outside observer. Interest group covers companies and NGOs, who have a publicly stated agenda on the topic. Users are officials working at ministries or agencies whose operations are authorised by the law and who are the potential users of the online surveillance capabilities. Politician refers to politicians and politically appointed officials, e.g. political advisors. Outside observer includes e.g. oversight organisations, researchers and journalists, that is, all the actors who are typically regarded as watchdogs or knowledge brokers.

Q-Factor Analysis

In contrast to a well-known R-factor analysis that aims to identify latent variables or factors behind the strongly associated items, Q-factor analysis focuses on the correlations between individuals. Therefore, Q-factor study requires a decent number of variables, which in our study are statement cards covering the concourse. Carefully selected statements in Q-factor analysis take the task of a representative sample of individuals in R-factor analysis. (Stephenson, 1935). In Q-type factor analysis individuals who sort the statement cards roughly the same manner load on the same factor. Typically, few different factors or point of views emerge from the analysis. These points of views are typically regarded as discourses, narratives or frames depending on the researcher's theoretical predilections. The factors highlight the extreme opinions, but also the areas of consensus on certain statements across the factors (e.g. Dryzek and Holmes 2002: 29). This indicates that respondents differ in terms of how they rank some statements, but also that they agree on the location of other statements in the grid.

We entered individually ranked Q-sorts into a computer software, the freely downloadable PQMethod[4], designed specifically for Q-methodology. Our final Q-factor analysis extracted four centroids, but one of them (3rd in row) was discarded because no individual loaded significantly on this factor. We applied Varimax rotation in order to create a factor solution in which participant's loading on one factor is maximised while its loading on other factors is minimised (Nummenmaa 2004: 346-347). Statistically significant factor loading at the level of 0.01 for a single factor was calculated by hand to be 0.39 (Brown 1980: 222-223). In total, 16 participants loaded exclusively on one of the final three factors that we named Frame 1: Balancing privacy and security (factor 1), Frame 2: Protecting human rights (factor 2) and Frame 3: Expanding surveillance powers (factor 3). Five individuals loaded on factor 1, seven on factor 2 and four on factor 3 (see Table 1).

The three-factor solution accounts for 54% of the overall variance and the manually calculated eigenvalues of each of the three factors exceeded the threshold value of 1.00 (Table 1; Watts and Stenner 2012: 105). There is a correlation (0.4436) between factors 1 and 3, but they are still different enough by their content to be interpreted separately. Nine of the respondents were confounding, which means that they loaded on two factors. Notably, the confounded participants were distributed between all factor pairs. Only one participant had a significant negative loading, as the individual No. 10 disagreed with factor 2 (see Table 1). The lack of negative loadings suggests that the viewpoints are not polarised and mutually exclusive. A high number of confounded participants may indicate the complexity of the issues and an aspiration to consider online surveillance from various angles. Confounding could even imply that the views may have more in common than anticipated. Furthermore, the stakeholders who agree with the principles common to two views have managed to balance two interests and may then function as mediators in the debate.

Table 1. Participants' loadings on factors after Varimax rotation.

Participant		Factors (Frames)		
Number	Category	1	2	3
1	Interest group	0.6084	-0.0040	0.4926
2	Interest group	**0.6806X**	0.2501	0.1746
3	User	0.3701	-0.1497	**0.6474X**
4	Politician	0.5246	0.5955	0.0429
5	User	0.5996	-0.1948	0.4122
6	User	**0.5438X**	0.1442	0.0017
7	Interest group	0.1574	**0.5888X**	0.2619
8	Politician	0.2409	-0.2379	**0.8354X**
9	Outside observer	0.4395	0.5138	-0.0303
10	Politician	0.0863	-0.6097	0.5401
11	Interest group	-0.0260	**0.7927X**	-0.0161
12	User	0.5673	0.0846	0.4210
13	Outside observer	0.3594	0.4064	0.5558
14	Interest group	**0.5014X**	-0.1148	0.2220
15	Outside observer	0.1729	0.3834	**0.5830X**
16	Interest group	**0.5903X**	0.2308	0.2507
17	Politician	0.0908	**0.8587X**	0.0852
18	User	0.1759	0.0899	**0.5740X**
19	Outside observer	0.0568	**0.6671X**	0.2232
20	Outside observer	0.2575	**0.6213X**	-0.2530
21	Outside observer	-0.0071	**0.7879X**	-0.1610
22	Outside observer	**0.6330X**	0.2207	0.2694
23	Outside observer	*0.4793*	*0.4027*	*0.3196*
24	Anonym	0.1854	**0.6781X**	0.1026
25	Politician	0.2952	0.2889	0.3885
Eigenvalue		4.25	5.5	3.75
Explained variance (%)		17	22	15
In total (%)			54	

Statistically significant differences (p < 0.01) are bolded and marked with an X as is conventional in Q-methodology.

The factor arrays and the 45 statements used in this study are introduced in Table 2. Factor array is “a single Q-sort configured to represent the viewpoint of a particular factor” (Watts and Stenner 2012: 140). The values (from 5 to -5 through 0) under each factor array show the configuration, in other words, an estimate, of how an ideal type of participant associated with the factor would have arranged the statements. Factor arrays are calculated from the weighted and standardised factor scores. Therefore, higher loadings have more influence on the configuration than lower ones. The confounded factor loadings were excluded from the factor arrays. The factors were interpreted by using respondents’ Q-sort rankings and elaborations presented in interviews regarding the statements. In the following, these three factors are described, interpreted and discussed in more detailed as three distinctive frames.

Table 2. The 45 statements with regard to the factor array.

	Statement	**Factor array (frames)**		
		1	**2**	**3**
1	Secure internet is a vital tool in a free and democratic society. The products and services in support of this should not be compromised by handing over decryption keys.	+5*	+3*	0*
2	Information requests from Law enforcement and Intelligence Agencies place an unreasonable burden on Internet based service providers.	-1	-2	-4*
3	Data from online surveillance should be deleted immediately after the case is closed, and should not be used for other purposes than it was collected for.	-1*	-1*	+1
4	New surveillance measures are introduced gradually, obscuring the totality of the extended powers over time	-2*	+1	+1
5	Surveillance methods most invasive of privacy, such as equipment interference, should only be reserved for the most serious criminal offences or serious threats of national security.	+2	+3	+1
6	In order to receive valuable information on national security threats, we must strengthen our international co-operation.	+4	+1*	+4
7	Expanding authorities' access to online communications will make society safer for citizens.	+3	-2*	+4
8	Radicalized people who are at risk of becoming violent, should be identified through their online behaviour and have their communication monitored.	+1*	-1*	+3*
9	Use of so called "network traffic intelligence" [information derived from global communications network cables] is an accurate and reliable way to uncover previously unknown threats to national security	-1*	-3*	+2*
10	The current security and crime situation justifies more comprehensive surveillance capabilities in cyberspace.	+4	-1*	+5
11	If you have nothing to hide, you need not be concerned about surveillance by the authorities.	-4	-5	+3*
12	One should only share intelligence with, or receive intelligence from, countries that follow the UN human rights convention.	0	+4*	0
13	Traditional (offline) surveillance methods have revealed what people do, accessing communications in the digital domain reveals what people think. There is a fundamental change in intrusion between the two actions.	-2	+2*	-1
14	The targeting of surveillance methods must not be discriminatory, i.e. they must not be based on race, religious beliefs, opinions, membership of a social group or other personal factors without just cause.	0*	+5*	+2*
15	Regardless of privilege, the communications of sensitive professions, such as lawyers, journalists or doctors, should be subject to surveillance if they are communicating with a person who poses a risk to national security.	0	-5*	+1
16	It is vital that people be accorded the same basic rights on networks as they have outside them.	+5*	+2	0
17	By increasing online surveillance as a consequence of terrorist attacks, we weaken the very ideals attacked by the terrorists.	0	0	-5*

18	The possibility of being under online surveillance leads to self-censorship and fear, ultimately suffocating democratic discussion and freedom of thought.	-1	-1	-5*
19	We must restrict what powers of surveillance we allow authorities to have now because we can't control how they might be used by future governments.	-4	+3*	-3
20	Agencies over rely on, and are over confident in the ability of digital communications surveillance.	0	0	-2*
21	Monitoring cross-border network communication is more acceptable than monitoring domestic communications.	-2	-2	0*
22	Our cross border digital surveillance is [/would be] based on filtering data against specific parameters before it is sent for analysis, therefore it is targeted, not mass surveillance.	+1*	-4*	+5*
23	The media has too much influence on public sentiment regarding online surveillance.	-3	-3	+2*
24	*Government authorities will get what they want regardless of the debate.*	*-4*	*-2*	*-3*
25	My country's approach to legislating online surveillance powers strikes the right balance between ensuring security and protecting privacy.	+4	-3*	+3
26	The intrusion into privacy happens when the data is collected/stored, it does not have to be looked at.	+2*	0*	-3*
27	*Criminals will always find ways around being detected by online surveillance, for example by moving to Internet Service Providers in other, less intrusive nations.*	*0*	*0*	*0*
28	Technology is advancing so quickly that authorities and the law are struggling to keep up.	+1	0	+4*
29	If the public are ok with their privacy being impinged for the sake of security, it is because they do not fully understand why privacy is so important in digital age.	-1	0	-4*
30	There is no difference in level of privacy intrusion between examining content of communications data and collating meta-data.	-3	+1*	-1
31	In matters of National Security, legislation regarding online surveillance should be decided by our government, not external powers such as the EU.	+3	-1*	-1*
32	A citizen should be informed afterwards if their online communications have been accessed, stored or used in investigation.	+1	+4*	+2
33	*Big data analysis of online communications will lead to poor decision making about individuals through misjudged inferences.*	*-2*	*-1*	*-2*
34	*Data retained by the service provider for law enforcement purposes should be kept for 12 months to allow investigative opportunities to be fully utilised.*	*-3*	*-3*	*-2*
35	It ceases to be targeted surveillance if it also captures data from those not communicating directly with the person under suspicion.	-2*	0*	-4*
36	*The public should be informed about the extent and outcome of online surveillance, on a sufficiently frequent and detailed basis, in order to uphold public trust in law enforcement and avoid suspicion that operations are wider reaching than they actually are.*	*+2*	*+2*	*0(*)*
37	The preventative effect of monitoring cross-border online communications offset all perceived financial or societal costs.	-5	-4	-1*

38	*To enable full democratic control, those who are responsible for the oversight and regulation of Secret Intelligence Agencies must have sufficient awareness of, and the technical competence to understand, all their capabilities and activities.*	*+3*	*+2*	*+3*
39	Fully independent control mechanisms are a more effective way of ensuring our rights are protected than trying to restrict or remove the capabilities available to authorities.	+2*	-4*	-1*
40	The current and proposed legislation on intelligence and digital surveillance measures is so ambiguous and fragmented that it is difficult to understand, and open to broad interpretation.	-5*	+1*	-3*
41	The courts should make an independent and full scope assessment for each warrant application, and should not rule simply on the basis of the applicants' judgement.	+3	+4	+2
42	The decision making process on warrants for monitoring cross-border network traffic should involve not only the judge and the intelligence agency but also an independent public interest advocate or such, in order to safeguard the rights and interests of those placed under surveillance.	+1	+5*	+1
43	Warrants for the use of spyware should include analysis of any possible damage the software may cause to a data system or process that it controls, as well as a plausible description of how the software can be removed without posing a risk.	0	+1*	-2
44	An anonymous, independent, legal channel for reporting misuse of secret powers must be guaranteed available at all levels to support staff without risk to themselves or national security.	+2	+3	0
45	*Authorisation processes involved in online surveillance can introduce further risk by unreasonably inhibiting or delaying important lines of investigative enquiry.*	*-3*	*-2*	*-2*

Statistically significant differences (p < 0.05) are marked with an asterisk. Consensus statements are in italics.

The Three Frames

Frame 1: Balancing privacy, freedom and security

The importance of the secure Internet in a free and democratic society (statement 1/ value +5; p < 0.01) and basic rights on networks (16/+5; p < 0.01) characterise Frame 1 (see Table 2 to read the full statements). Five individuals loading on this factor consist of three interest group representatives, one user and one outside observer. These interviewees consider the extension of online surveillance capabilities necessary in the present security and crime situation (10/+4). They evaluate that the aims of ensuring security and protecting privacy are balanced in the current and proposed legislation (25/+4). They feel that the intelligence legislation draft has been clearly formulated (40/-5; p < 0.01). Informants forming this frame strongly disagree that gathering network traffic intelligence through tapping the cables, would compensate for all the costs (37/-5), but in general, they believe that the extension of authorities' surveillance powers will make Finnish society more secure for its citizens (7/+3). According to the post-sort interviews, some of the respondents reasoned that expectations towards network traffic intelligence, being only one of the available surveillance techniques, were too high. Participants seem to have confidence in democratic society and policy debate, but they also emphasise the need to ensure rights to privacy, because everybody has something to hide (11/-4). These individuals do not believe that future governments would pose a risk as to why Finland should limit its online surveillance capabilities now (19/-4). They believe that legislation is shaped through policy debate (24/-4) and think that the media has not had too much influence on the public sentiment towards online surveillance (23/-3). This set of individuals is characterised by their approval of all positive statements about the oversight and control of law enforcement agencies' capabilities (e.g., 36, 38, 39, 41 and 44).

Informants loading on factor 1 seem to evaluate online surveillance by contextualising it within the larger picture of regulating and protecting cyberspace. They balance privacy and liability, that is, they regard that people have a right to privacy in cyberspace, but not without responsibility for their own online behaviour. Thus, authorities should also be able to respond to criminality and other threats in cyberspace. To balance authorities' powers, however, they call for accountability and public evidence of fair surveillance practices through oversight and control mechanisms. Some informants also view cyberspace as a platform for business and authorities should not interfere with it too much, for example, by requiring backdoors in software. On the issues of national security, they think that states should have legislative power over online surveillance instead of supra-state organs, e.g. the EU (31/+3; $p < 0.01$).

Despite valuing privacy, human rights in general seem not to elicit the strongest opinions among the individuals loading on this factor, but they tend to locate the statements involving human rights around the middle of the grid. For example, in column zero, there are statements relating to discrimination (14; $p < 0.05$), protecting communication of certain privileged professions such as lawyers and doctors (15) and sharing intelligence only with countries following the UN human rights convention (12). Post-sort interviews revealed that the reasoning behind neutral positions or mixed feelings towards certain statements regarding human rights were due to recognising value in often antagonistic viewpoints, and therefore being unable to choose one or the other of the competing options. For example, although it is important to protect the communication of certain professions, it could lead to loopholes in legislation if protection is taken to extremes. Another paradoxical situation arises when useful intelligence to protect Finnish society lies in the hands of a country where human rights do not meet UN standards. Some of the participants argued that Finland should not refrain from preventing, e.g. terror attacks in those countries, if sharing intelligence achieves good.

Only this group of participants somewhat agreed that an intrusion into privacy happens immediately when the information is collected, even though it has not yet been looked at (26/+2; $p < 0.01$). In the post-sort interviews, many holders of this view seemed to respect that the Finnish system of network traffic intelligence will be based on filtering the real-time data flows, instead of enabling retrospective retrievals by storing all data. Despite that, these individuals were the most sceptical towards the promise of deleting the collected data immediately after the case is closed (3/-1; $p < 0.01$). One explanation for that was that the intelligence cycles of military intelligence can be around 25 years.

Frame 2: Protecting human rights

Individuals loading on Frame 2 value human rights and fundamental freedoms. This group consists of three outside observers, two interest group representatives, a politician, and one who did not disclose their background. These respondents agree that surveillance techniques must be non-discriminatory (14/+5, $p < 0.01$) and that people's rights in the surveillance process must be safeguarded by reliable mechanisms (42/+5, $p < 0.01$; 41/+4; 32/+4, $p < 0.01$). Furthermore, these individuals insist that intelligence should be only shared with or received from countries that follow the UN's convention on human rights (12/+4, $p < 0.01$). They highlighted in the interviews that intelligence exchange is a complex issue highly dependent on the situation. For example, one respondent described the authorities' current mandate of discretion as being too wide and called for firmer political control of information exchange with questionable countries.

The participants' strong emphasis on human rights becomes visible in their strong disagreement with certain statements. They wish to protect communication of certain professional groups, such as doctors and journalists, from online surveillance (15/-5, $p < 0.01$). They disagree that people who have nothing to hide, do not need to concern themselves about surveillance by the authorities (11/-5). People leaning to this frame, are somewhat sceptical towards network traffic intelligence as a technique. They have doubts that, network traffic intelligence may be or may turn into mass surveillance (22/-4, $p < 0.01$) and have doubts about its effectiveness (37/-4), accuracy and reliability (9/-3, $p < 0.05$). However, despite the low weighted average received for statement 22 on mass surveillance, the respondents talked about mass surveillance surprisingly little in post-sort interviews, and when they did, mass surveillance did not represent a rationale. Instead, participants demonstrated awareness of the problems related to usage of such a vague, charged, and potentially misleading indication. Participants holding this view also seem to have some concerns about and mistrust towards the online surveillance powers of future authorities. Firstly, they somewhat agree that Finland should limit the surveillance capabilities now, because nobody knows how future governments may use them (19/+3, $p < 0.01$). They disagree (39/-4, $p < 0.01$) with the idea that independent safeguard and oversight mechanisms would be more efficient to ensure our rights rather than removing or restricting authorities' current powers. Secondly, contrary to individuals loading on Factors 1 and 3, these stakeholders are slightly uncertain both whether expanding authorities' online surveillance capabilities would improve Finland's security (7/-2, $p < 0.01$) and about justifying the expansion through the current security situation (10/-1, $p < 0.01$). Post-sort interviews showed that these respondents were concerned of having not enough information about the utility of expanded online surveillance capabilities for improving security. Therefore, raising questions on effectiveness, usefulness and impacts of online surveillance can be interpreted as efforts to gain more information.

Only the individuals loading on factor 2 assess that security may have gained an upper hand at privacy's expenses (25/-3; $p < 0.01$) in the legislation. However, in post-sort interviews, many of them expressed the belief that the intelligence legislation proposal has improved significantly during the process, and the main concerns seemed to be in the details instead of general questions.

Frame 3: Expanding surveillance powers

Individuals gathering around Frame 3 concentrate on explaining and justifying why Finland would need to expand its online surveillance capabilities. The interviewees loading on this factor were two users, one politician and one outside observer. Foremost, they consider that the current security threats justify more comprehensive surveillance methods in cyberspace (10/+5) and highlight the fact that new proposed legislation would not be mass surveillance (22/+5, p < 0.01). Furthermore, they argue that the authorities' wider access to online communication will improve society's security (7/+4), although authorities and legislation will have challenges to keep up with quickly developing technologies (28/+4, p < 0.01). These respondents also believe that strengthening international co-operation would help Finland receive valuable information on national security threats (6/+4).

On the other hand, individuals loading on factor 3 firmly believe that online surveillance would not suffocate democratic debate (18/-5, p < 0.01), or that expanded powers would not weaken democratic values that terrorists are trying to undermine (17/-5, p < 0.01). They consider that service providers will not be burdened unreasonably by authorities' information requests (2/-4, p < 0.05) and that capturing information from third parties would still be targeted rather than mass surveillance (35/-4, p < 0.01). These individuals also disagree with arguments that an intrusion into privacy happens as early as when the data are collected but not looked at (26/-3, p < 0.01) and that the proposed intelligence legislation would be too difficult to interpret (40/-3, p < 0.05).

This group of respondents is the only one that agrees with the statement that people who have nothing to hide do not need be concerned about authorities' surveillance (11/+3; p < 0.01). The interviews provided further information for understanding why some individuals agreed with the statement while the majority of all respondents opposed it strongly; they considered that the improved oversight and control mechanisms will be able to detect potential attempts to misuse intelligence data. Furthermore, respondents estimated the amount of data so remarkable that non-relevant communication was seen rather as a burden or failure instead of something interesting. They also emphasised that according to the law proposal, non-relevant data must be deleted. Therefore, people should not be worried about dishonest officials misusing intelligence data or the system collating the communications of law-abiding citizens.

People associating with this frame tend to have more positive attitudes (9/+2; 37/-1; p < 0.01) towards network traffic intelligence as a technique than the other groups. Nevertheless, their estimations of the efficacy of the technique are quite cautious in post-sort interviews, since the technique was not yet in use. Even so, they seemed confident that the new technique would improve authorities’ capability.

The Common Ground between the Frames

Despite having different frames on surveillance, the three stakeholder groups are also very close to each other with respect to a number of important statements (Table 2, p < 0.05 in italics). However, such statements do not necessarily elicit the strongest feelings. For example, the only statement (27) that receives a value of zero from all the groups suggested that criminals would always find ways around being detected from online surveillance. Post-sort interviews showed that the statement was agreed on but found to be non-relevant: online surveillance is not futile even though some criminals may escape from authorities. All respondents agreed that the public debate is important and will shape legislation (24/factor 1:-4, factor 2:-2, factor 3:-3). Three of the consensus statements are related to the need for oversight mechanisms and safeguards for online surveillance measures. For example, participants are unanimous about the idea that the authorisation process involved in online surveillance will not introduce further risks by unreasonably inhibiting or delaying important lines of investigative enquiry (45/f1:-3, f2:-2, f3:-2). Respondents consider that the authorisation process is quick enough and see that potential problems will relate only to the design or some other reasonable or acceptable technical details. Informants also think that, to enable full democratic control, those who are responsible for the oversight and the regulation of secret intelligence agencies must have sufficient awareness of and the technical competence to understand all surveillance capabilities and activities available to agencies (38/f1:3, f2:2, f3:3). Informing the public about the extent and outcome of online surveillance seems to be, in a statistical sense, an interesting borderline case for the third factor (36/f1:2, f2:2, f3:0), since the statement is included in both the calculation of the consensus statements and the distinctive statements. Interviews show that several respondents, despite the factor they sit on, consider that annual intelligence reports in Norway, Sweden and Estonia, provide adequate information to the public.

The statement about data retention (34/f1:-3, f2:-3, f3:-2) was met with somewhat mixed interpretations, since only some respondents recognised that it was not related to the intelligence legislation proposals, but operators' existing obligation to store data for authorities.

The Next Steps of the Finnish Policy Debate on Online Surveillance

The frames unravel the debate

We analysed 25 stakeholders' views on the police and intelligence agencies' online surveillance capabilities and the proposed expansion of them. Through Q-factor analysis and the analysis of recorded post-sort interviews, we extracted three frames that we called Balancing privacy, freedom and security, Protecting human rights, and Expanding surveillance powers. Together these frames illustrate the Finnish policy discussion of online surveillance, and also point out, as anticipated, latent dimensions such as values and interests under the surface of the public debate (van Eeten 2001a; Pirkkala 2017).

Our analysis explicated that the three frames have deal-breakers that are rooted in rather fixed and stable interests and values, which go beyond attitudes towards individual statements and sometimes, beyond background or position too. Furthermore, the specific strength of Q-research protocol lies in its capacity to discern which of the particular statements are the most significant for each frame. Changing those fundamentals may be hard, even impossible, and perhaps not necessary. Instead, learning to respect and accept that specific concerns and more general values or interests sustaining these must have a legitimate place in the online surveillance debate should it provide a more sustainable decision-making process in the spirit of deliberative democracy (see e.g. Cohen 1997; Setälä 2014). By respect and acceptance, we mean an ability to relate various perspectives in a manner that seeks solutions. The deal-breaker for Frame 1 is a perception that, on the one hand, people have right to protect themselves online, but on the other hand, the authorities have a responsibility to provide security for the people. Therefore, cybersecurity must not be weakened on either fronts by any means. Individuals forming Frame 2 emphasise the importance of human rights, especially non-discrimination and the protection of the weak and the vulnerable in society. Finally, Frame 3 highlights that security authorities exist for the benefit of society and citizens, not against them. Authorities can fulfil their duty to maintain security, only if they have access to adequate online surveillance capabilities.

Perhaps even more important lesson than discovering latent frames and related specific concerns is the capability of Q-methodology to highlight so called ambiguous issues and common ground. Our findings suggest both ambiguous issues and common ground as potential openings for developing the online surveillance debate further. Ambiguous issues are matters that the debaters acknowledged with mixed feelings or opinions based on assumptions. Participants' positions on ambiguous issues seem more open and therefore the debaters are ready to hear new evidence to reason their stance. This is consistent with the principles of reasoned and inclusive discussion that considers all relevant information suggested by deliberative democracy. Furthermore, we argue that it is important to follow-up on ambiguous issues later, after Finland has enough experiences of how intelligence legislation operates. Practical examples of such questions come especially from Frames 1 and 2:

- What are the pros and cons of network traffic intelligence? How does it work as a tool and complements other intelligence gathering techniques?
- Are the financial costs of online surveillance manageable?
- It is understandable, if the new legislation does indeed need to be improved. Could the authorities elaborate openly on what kinds of amendments would be necessary, and why?
- Have the authorities found a way to open up a bit more about intelligence activities in Finland—not at the level of tactics, but more general information for the citizens and stakeholders?
- Have the authorities been able to look after the rights of individuals whose communication has been under surveillance? Is there any public evidence of that available? Do the legislated safeguards work?
- How targeted has the network traffic intelligence gathering been and does it threaten to slip towards "mass surveillance"?

An area of consensus emerged from the shared views and thoughts among the respondents. Statements falling into this area may not elicit the strongest sentiments, but they constitute a common ground on which further agreement could be built (see e.g. van Eeten 2001a). Delightedly, the statement "Government authorities will get what they want regardless of the debate" was rejected in all frames. The statement was regarded false, because all saw that public debate does matter, and the legislative process has already shown this. Stakeholders agreed that the online surveillance has to be accountable and legitimate and thus requires robust oversight mechanisms and safeguards and technically competent individually to carry out these tasks.

Stakeholders facilitate the debate

Our results support the view that experts do have an important role in deliberating complex policy issues where citizens' direct involvement may be challenging (Gutmann & Thompson 2004). We recognized a certain "function" for each frame in the debate. Frame 3 is clearly advancing the intelligence legislation in the name of security, whereas Frames 1 and 2 are balancing the ambition to expand surveillance by constantly reminding us about the importance of human rights and privacy, the fragility of cybersecurity, the complexity of technology, uncertainty about the surveillance efficiency, and possible negative effects on business. Despite highlighting some ambiguous issues, Frame 1 tends to approve the new legislation. Frame 2, however, shows more reservations.

We argue that addressing the specific concerns by each frame moves the policy deliberation forward and improves the legitimacy of authorities' capabilities. Responding to stakeholders' questions is mostly a responsibility of those who use the new capabilities and supervise their usage, because they have access to the information. The security authorities, respective ministries and the newly established oversight-bodies, the Intelligence Ombudsman, and the parliamentary Intelligence Oversight Committee, are in a crucial position to provide sufficient information for assessing the effectiveness and legality of the new surveillance practices. To protect citizens against the abuses of power, authorities are responsible for appropriate actions as defined in the legislation and must be able to justify and show the results of their decisions and practices. People are more willing to confer legitimacy upon the authorities if they can be trusted to carry out activities professionally and effectively while also treating individuals impartially.

It is also important to clarify to the debaters that some issues previously regarded ambiguous have been solved during the process. These arguments are extremely useful reminders that through democratic, rational and tenacious discussion, disagreements can often be settled in a manner that is satisfactory, even if not perfect, for all the parties involved. For example, instead of objecting the proposed legislation simply as mass surveillance, which was central in the first working group report (Puolustusministeriö 2015), participants now showed frustration and avoidance towards the vague concept and rather discussed on exact wordings of the law proposals. Furthermore, a discourse which considered non-regulation as an advantage (Sirkkunen and Haara 2017) was replaced by a discourse that intelligence legislation increases predictability and openness, which is a benefit for society and business. Clearly, the business sectors' concerns were met with an adequate response, and support was gained, which likely is the result of inclusion of a business representative in the preparatory working group.

We argue that the general elements of legitimate and sustainable online surveillance system can be derived from many sources, e.g. from ECtHR judgements, reports and research (e.g. Cayford and Pieters 2018; Shiraz 2017; RUSI 2015; Lyon 2015; 2007[5]), but the crux of the matter is to adjust the general principles into country specific conditions and concerns through local stakeholder involvement. Deliberative democracy presupposes that participants seek acceptable solutions together through reasoning, are willing to consider each other’s viewpoints and, when necessary, able to make concessions for the common good (e.g. Bächtiger et al. 1998; Cohen 1997; Dryzek 2000; Setälä 2014). Q-methodology promises to uncover those viewpoints and their constituents and therefore can potentially improve deliberation. This approach seems to be applicable particularly in the Nordic countries with a strong tradition of coalition governments, rational planning and stakeholders' interests (see, e.g. Kettunen 2001).

Implications for research and practice

By focusing on the emerging online surveillance legislation in Finland, our study contributed to online surveillance policy research. In addition, we demonstrated that Q-methodological research could feed policy discussion in the spirit of deliberative democracy. Finally, we also raised some substantive questions about online surveillance in Finland that need to be answered in the future.

The framework of deliberative democracy we employed suggests that people who experience the consequences of policy decisions should be engaged in discussions. Furthermore, the discussion should be regular, because the decisions, for example legislation, need re-assessing and upgrading every now and then. . Once the discussion continues, Q-methodology could be a convenient tool for uncovering fundamental viewpoints, but also dissecting the specific problems that need further discussion.

Our study offered a detailed empirical analysis on online surveillance debate in Finland. However, in addition to national case studies, we encourage country comparisons that would address how international guidelines and recommendations are perceived beyond the national laws and policies. Are the debates framed similarly in different countries? What are the most controversial issues in each country? Research should include also the citizens’ perceptions of online surveillance policy. In such research, qualitative design might be more faithful to the principles of deliberation by letting people to formulate opinions using their own expressions and terminology. This would also allow an examination whether, for example, competencies form barriers to participate in the surveillance debate.

With regard to the advancement of policy discussion, our study leads the way for constructive debate by addressing frame-specific concerns, ambiguous issues and common ground. The most important follow-up questions that were raised by the stakeholders are the effectiveness and legitimacy of the Finnish surveillance system – oversight mechanisms included – and practice. If there is not information available about the national surveillance practices and achieved results, people will fill in the gaps by their own assumptions or international examples perceived from the media, which may be incompatible with the current legislation. This would only confuse, not clarify the debate.

Based on the feedback we received from the interviewees, we are quite confident that the Q-methodological research design encouraged many of the Finnish key stakeholders to unexpected self-reflection. The advantage of a Q-methodological card-sorting interview is that it allows respondents to express not only their personal views but also prompts them to determine the relative salience of all items related to the online surveillance debate as a whole (Clarke 2007). Thus, Q-research feeds self-reflection and may eventually broaden the key stakeholders' understanding of the issues and other perspectives. Certainly, more research is needed. In particular, we suggest testing whether Q-methodology could support an ongoing policy process in goal-oriented way, as a systematic part of real policy deliberation.

Acknowledgements

The research is part of the international, comparative research project "Taking Surveillance Apart? Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers". Authors are grateful to Dr Guro Flinterud and Amy Humphrey for their contribution to development of the research instrument. Authors also would like to thank the anonymous reviewers for valuable comments that improved the quality of the paper.

Funding

This work was supported by NordForsk under Grant 80895.

References

Arter, D (2006) *Democracy in Scandinavia. Consensual, Majoritarian or Mixed?* Manchester: Manchester University Press.

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon & R.B.J. Walker (2014) After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8: 121–144.

Bächtiger, A., J.S. Dryzek, J. Mansbridge & M.E. Warren (2018) The Oxford Handbook of Deliberative Democracy. Oxford: Oxford University Press.

Bernal, P. (2016) Data Gathering, Surveillance and Human Rights: Recasting the Debate. *Journal of Cyber Policy* 1(2): 243–264.

Brown, S.R. (1980) *Political Subjectivity*. New Haven, CT: Yale University Press.

Cayford, M., & W. Pieters (2018) The Effectiveness of Surveillance Technology: What Intelligence Agencies Are Saying? *The Information Society* 34: 88–103. https://doi.org/10.1080/01972243.2017.1414721

Clarke, S.E. (2007) Context-Sensitive Policy Methods. In *Handbook of Public Policy Analysis: Theory, Politics and Methods*, eds. F. Fischer, G.J. Miller and M.S. Sidney. Boca Raton: CRC Press, 443–61.

Cohen, J. (1997) Deliberation and Democratic Legitimacy. In *Essays on Reason and Politics. Deliberative Democracy,* eds. J. Bohman and W. Rehg. Cambridge: MIT Press, 67–91.

Durning, D.W., & S.R. Brown. (2006) Q Methodology and Decision Making. In *Handbook of Decision Making,* ed. G. Morçöl. Boca Raton: CRC Press, 537–63.

Dryzek, J.S. (2000) *Deliberative Democracy and Beyond. Liberals, Critics, Contestations*. New York: Oxford University Press.

Dryzek, J.S., & L.T. Holmes (2002) *Post-Communist Democratization. Political Discourses across Thirteen Countries.* Cambridge: Cambridge University Press.

Ellis, G., J. Barry & C. Robinson (2007) Many Ways to Say 'No', Different Ways to Say 'Yes': Applying Q-Methodology to Understand Public Acceptance of Wind Farm Proposals. *Journal of Environmental Planning and Management,* 50(4): 517–551.

Ericson, Richard V., & K.D. Haggerty (1997) *Policing the Risk Society*. Oxford: Clarendon Press.

FRA (2017) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*. FRA. European Union Agency for Fundamental Rights. Luxemburg

Gutmann, A., & Thompson, D. (2004) *Why Deliberate Democracy?* Princeton University Press: Princeton.

Habermas, J. 1984. *The Theory of Communicative Action*. Volume I. Reason and the Rationalisation of Society. Boston, MA: Beacon Press.

Head, B.W., & J. Alford (2015) Wicked Problems: Implications for Public Policy and Management. *Administration & Society,* 47(6): 711–739.

Hintz, A., & I. Brown (2017) Enabling Digital Citizenship? The Reshaping of Surveillance Policy after Snowden. *International Journal of Communication* 11: 782–801.

Kettunen, P. (2001) The Nordic Welfare State in Finland. *Scandinavian Journal of History* 26(3): 225–47.

Kortesoja, M., R. Kunelius & H. Heikkilä (2019) Lyhyt matka epäisänmaallisuuteen. Valtion ja median suhteet HS:n tietovuotoa koskevassa keskustelussa. *Media & viestintä,* 42(2): 76–98.

Kreissl, R., & D. Wright (2015) Surveillance in Europe. Routledge.

Leigh, I., & N. Wegge (2019) Intelligence and Oversight at the Outset of the Twenty-First Century. In *Intelligence Oversight in the Twenty-First Century. Accountability and Changing World,* eds. I. Leigh and N. Wegge. Studies in Intelligence. London: Routledge, 7–24.

Lehtonen, P., & P. Aalto (2016) Policy Requirements for Automated Border Control System: A Q Methodological Study of Finland in the Context of a Large European Research Project. *Operant Subjectivity: The International Journal of Q Methodology,* 38(2): 1–14. DOI: 10.15133/j.os.2016.004

Lemieux, F. (2019) *Intelligence and State Surveillance in Modern Societies. An International Perspective.* Bingley: Emerald Publishing Limited.

Liikenne- ja viestintäministeriö (2014) *Digitaalisen yhteiskunnan tulevaisuus*. Liikenne- ja viestintäministeriön edustajan eriävä mielipide tiedonhankintalakityöryhmän mietintöön. In Puolustusministeriö (2015), Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. Liite 3 [Appendix 3]. https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf [accessed December 12, 2018].

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

Lyon, D. (2015) *Surveillance after Snowden*. Cambridge: Polity.

Murakami Wood, D., & C.W.R. Webster (2009) 'Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example'. *Journal of Contemporary European Research,* 5(2): 259–273.

Murray, D., & P. Fussey (2019) Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review,* 52(1): 31–60.

Nummenmaa, L. (2004) *Tilastolliset menetelmät*. Helsinki: Tammi.

Oikeusministeriö [The Ministry of Justice] (2017) Tiedustelutoiminnan valvonta. [Oversight of Intelligence Gathering]. Mietintöjä ja lausuntoja [Deliberations and Reports] 18/2017. http://urn.fi/URN:ISBN:978-952-259-576-8 [accessed August 14, 2019]

Omand Sir D., & M. Phythian (2013) Ethics and Intelligence: A Debate, *International Journal of Intelligence and Counter Intelligence,* 26(1): 38–63. DOI:10.1080/08850607.2012.705186.

Pirkkala, S. (2017) Mikä tekee luonnon monimuotoisuuden köyhtymisen pysäyttämisestä Suomessa pirullisen ongelman? *Politiikka,* 59(1): 33–51.

Puolustusministeriö [Ministry of Defence] (2015). Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. [Guidelines for Developing Finnish Legislation on Conducting Intelligence. A Report of the Working Group] https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf [accessed December 12, 2018].

Puolustusministeriö [Ministry of Defence] (2017). Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Työryhmän mietintö. [Proposal for legislation on military intelligence. Working group report]. Puolustusministeriö [Ministry of Defence], 2017. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79757/PLM_Ehdotus%20sotilastiedustelua%20koskevaksi%20lainsaadannoksi.pdf [accessed August 14, 2019]

Rawls, J. 1996. *Political Liberalism*, 2nd edition. New York: Columbia University Press.

Rein, M., & D. Schön (1996) Frame-Critical Policy Analysis and Frame-Reflective Policy Practice. *Knowledge and Policy,* 9(1): 85–104.

Rittel, H.W.J., & M.M. Webber (1973) Dilemmas in a General Theory of Planning. *Policy Sciences,* 4: 155–169.

Richards, N. (2013) The Dangers of Surveillance. *Harvard Law Review*, 126: 1934–1965.

Rosenberg, S. (2014) Citizen Competence and the Psychology of Deliberation. In *Deliberative Democracy. Issues and Cases*, eds. S. Elstub and P. McLaverty. Edinburgh: Edinburgh University Press, 98–117.

RUSI. (2015) *A Democratic Licence to Operate.* Report of the Independent Surveillance Review. Available at: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf [accessed July 8, 2019].

Schön, D., & M. Rein (1994) *Frame reflection. Exploring New Approaches to the Resolution of Policy Controversies*. New York, NY: Basic Books.

Setälä, M. (2014) The Public Sphere as a Site of Deliberation: an Analysis of Problems of Inclusion. In *Deliberative Democracy. Issues and Cases,* eds. S. Elstub and P. McLaverty. Edinburgh: Edinburgh University Press, 149–165.

Shiraz, Z. (2017) Globalisation and Intelligence. In *The Palgrave Handbook of Security, Risk and Intelligence,* eds. R. Dover, D. Huw and M. Goodman. London: Palgrave, 265–280.

Sirkkunen, E., & P. Haara (2017) *Yksityisyys ja notkea valvonta. Yksityisyys ja anonymiteetti verkkoviestinnässä -hankkeen loppuraportti*. Journalismin, viestinnän ja median tutkimuskeskus. Tampere: Tampereen yliopisto. http://tampub.uta.fi/bitstream/handle/10024/100510/978-952-03-0331-0.pdf?sequence=1&isAllowed=y [accessed April 5, 2019].

Sisäministeriö [The Ministry of Interior] (2017) Ehdotus siviilitiedustelua koskevaksi lainsäädännöksi. Työryhmän mietintö. [Proposal on Civilian Intelligence Legislation. Working Group Report.] 8/2017. http://urn.fi/URN:ISBN:978-952-324-129-9 [accessed August 14, 2019]

Sivan-Sevilla, I. (2019) Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968–2018. *Policy & Internet*, 11: 172–214, https://doi.org/10.1002/poi3.189

Stephenson, W. (1935) Correlating Persons Instead of Tests. *Journal of Personality,* 4(1): 17–24.

Stephenson, W. (1978) Concourse Theory of Communication. *Communication,* 3: 21–40. Chicago: The University of Chicago Press.

Stephenson, W. (1950) A Statistical Approach to Typology: The Study of Trait-Universes. *Journal of Clinical Psychology,* 6: 26–38.

Tiainen, M. (2019) Negotiating Digital Surveillance Legislation in Post-Snowden Times. An Argumentation Analysis of Finnish Political Discourse. *Journal of Language and Politics,* 18(2): 207–30. DOI: https://doi.org/10.1075/jlp.18004.tia

Wahl-Jorgensen, K., L.K. Bennett & J. Cable (2017) Surveillance Normalization and Critique. *Digital Journalism*. 5(3): 386–403. DOI: 10.1080/21670811.2016.1250607.

van Eeten, M.J.G. (2001a) Recasting Intractable Policy Issues: The Wider Implications of The Netherlands Civil Aviation Controversy. *J. Pol. Anal. Manage.*, 20: 391–414, https://doi.org/10.1002/pam.1000 van Eeten, M.J.G. (2001b) "Deliberative Democracy. The Challenge Ahead for Deliberative Democracy: in Reply to Weale." *Science and Public Policy,* 28(6): 423–426.

van Hulst, M., & D. Yanow (2016) From Policy "Frames" to "Framing": Theorizing and More Dynamic, Political Approach. *American Review of Public Administration,* 46(1): 92–112.

Vesa, J., A. Kantola & A.S. Binderkrantz (2018) A Stronghold of Routine Corporatism? The Involvement of Interest Groups in Policy Making in Finland. *Scandinavian Political Studies,* 41(4): 239–262. https://doi.org/10.1111/1467-9477.12128

Watts, S., & P. Stenner (2005) Doing Q Methodology: Theory, Method and Interpretation. *Qualitative Research in Psychology,* 2: 67–91.

Watts, S., & P. Stenner (2012) *Doing Q Methodological Research. Theory, Method and Interpretation*. London: Sage.

Notes

[1] E.g. Weber and Saravia v. Germany no. 54934/00; Liberty and Others v. the United Kingdom no. 58243/00; Szabó and Vissy v. Hungary no. 37138/14 ; Zakharov v. Russia 47143/06 ; 10 Human Rights Organisations v. the United Kingdom nos. 58170/13, 62322/14 and24960/15.

[2] Our unpublished interview study (N=20) suggests that students and staff of Finnish universities seemed quite unaware of intelligence legislation and its effects after it had entered in force.

[3] A Newspaper source: https://yle.fi/uutiset/osasto/news/secret_services_cyber_spies_twice_penetrated_foreign_ministry/7334589

[4] PQMethod is software by Peter Schmolck http://schmolck.org/qmethod/downpqwin.htm [accessed April 8, 2019]

[5] See endnote 1 for the ECtHR judgements.