Eur J Secur Res (2016) 1:115–133
DOI 10.1007/s41125-016-0007-z

ORIGINAL ARTICLE

"Accepting the Rules of the Game": Institutional Rhetorics in Legitimizing Surveillance

Roman Pauli[1] · **Hares Sarwary**[2] · **Peter Imbusch**[2] · **Tim Lukas**[2]

Received: 3 May 2016 / Accepted: 10 August 2016 / Published online: 24 August 2016

Abstract In this contribution, we analyze a comprehensive set of rhetorical strategies used by security professionals to legitimize the implementation of advanced surveillance systems. Drawing on a set of semi-structured in-depth interviews with experts from safety and security departments of an air traffic control provider in Italy, we show that both the expressed demands for surveillance as well as the rhetorical strategies used to legitimize its enforcement are embedded in dedicated institutional frameworks. We argue that institutions both facilitate and constrain their members' discursive actions to rationalize surveillance according to the institutions' vested interests. This intersubjective (re-)construction of an institution's social values is an important precondition for successful speech acts of securitization, in which the acceptance of exceptional measures is called into action to deal with potential threats.

Keywords Legitimization · Surveillance · Technology · Securitization

1 Introduction

To protect the citizens of the European Union from threats such as terrorism, natural disasters and crime, the European Commission invested in research and development under the security theme of the Seventh Research Framework Programme (FP7) until the end of 2013. Amongst others, the application of new technologies in

✉ Roman Pauli
roman.pauli@krimd.nrw.de

[1] Kriminologischer Dienst des Landes Nordrhein-Westfalen, Fritz-Roeber-Str.2, 40213 Düsseldorf, Germany

[2] Bergische Universität Wuppertal, Fakultät 2 Soziologie, Gaußstraße 20, 42119 Wuppertal, Germany

the field of civil security like intelligent surveillance or the integration, interconnection and interoperability of security systems was emphasized to protect the security of citizens, infrastructures and utilities (European Commission 2006). Under FP7, the European Security Research Programme was granted a total amount of 1.4 billion Euros between 2007 and 2013. Although intentionally dedicated to benefit the EU citizens, a review of security measures in FP7 requested by the Committee on Civil Liberties, Justice and Home Affairs concludes "that security research has only partly addressed the concerns of EU citizens and that security research has been mainly put at the service of industry rather than society" (Bigo et al. 2014: 1). The report further examines that this may be a result of the unequal representation of industry, security agency and civil society in the policy-making process. Most of the projects funded under the FP7 security theme were strongly technologically driven while at the same time a thorough assessment of legal, political and societal issues to determine their impact and effects rather tended "to focus on enhancing the impact and effectiveness of security technology in terms of societal acceptance, sidestepping issues linked with their legitimacy" (Bigo et al. 2014: 7). As far as issues touching fundamental freedom rights are "reduced to a matter of commercial considerations and as a limit to the acquisition of otherwise high-performance products" (ibid.), the underlying principle of a democratic legitimization of multi-billion expenses by EU citizens is hardly challenged. This is in line with the European Commission's recognition of problems associated to the societal acceptance of security technologies which may result in negative consequences: "For industry it means the risk of investing in technologies which are then not accepted by the public, leading to wasted investment" (European Commission 2012: 5).

Ideally, those in charge of the development or implementation of any new security measure have to align themselves to the concerns and criticism of those who may be affected by subsequent surveillance. In the light of the aforementioned conclusion drawn from the review on FP7 security measures, security advocates face the necessity to justify the legitimacy of surveillance. By doing so, they rely on a comprehensive repertoire of commonly used rhetorical strategies to defend their core business of surveillance. This may be the case when surveillance is scandalized in public debates on pros and cons of ideas, norms, actors and institutions (Schulze 2015).

In this article, we show that patterns of surveillance legitimization are to be found in various discourses beyond public scandalization wherever security advocates feel to be confronted with a necessity to justify their core business of surveillance. We argue that the patterns used to legitimize surveillance are subordinated to specific institutional norms and values, reinforcing the attitudes the members of an institution have towards surveillance. We, furthermore, examine how negotiations on the legitimacy of surveillance are structured hierarchically, depending on the very context of surveillance in which different agents argue for their vested interests.

Based on Schulze's (2015) recent elaboration on patterns of surveillance legitimization in the German discourse on the NSA scandal, we compile a set of basic rhetorical strategies to be found in various discourses on legitimization. In

addition, we draw on findings from organizational sociology to examine institutional norms that help to form what can be called context-specific security cultures. With the conclusion that a high-level overview on very basic rhetorical strategies to be found in any legitimization discourse can only be a starting point, we further examine the need for case-specific and detailed analysis. Following the introduction and our methodological approach, findings from our qualitative content analysis of interviews with experts from safety and security departments of an air traffic control (ATC) provider in Italy are presented. The article concludes with a discussion of the results and some indications for further research.

2 Surveillance Technology and Legitimacy in Institutional Frameworks

In recent years, concerns about security have acquired increasing importance for modern societies. A growing societal orientation towards threats and dangers has led to new approaches for protecting national and personal security. Besides expanding safety legislation and the implementation of novel security partnerships, technological innovations are at the core of this development. Increased access to and use of information and communication technologies has enabled new methods of surveillance and social control (Marx 2002), which can be summarized as "surveillance-oriented security technologies (SOSTs)" (Pavone and Degli Esposito 2012). According to Degli Esposito and Santiago Gómez (2015: 437), SOSTs are "technologies which collect information about the general population to monitor the activities of potential suspects and to prevent criminal acts from occurring." While expected to enhance the actual level of security, these technologies exercise an increasing amount of permanent surveillance on ordinary citizens and often conflict with privacy and fundamental freedoms. Particularly when implemented in institutions dealing with the protection of critical infrastructures from external and internal threats, SOSTs generate a serious pressure on employees that is difficult to escape.

Against this background, Renn (2005) distinguishes between various technology areas that are characterized by different acceptance criteria. While the acceptance of products and everyday technologies is merely based on a simple distinction of purchase or non-purchase, the acceptance of security technologies at the workplace can be judged by the extent to which they are being circumvented or even undermined. Associated conflicts affect less the quality and liability of a certain product, but rather the possible non-use of technologies that are perceived as too complicated and burdensome. Bonß and Wagner (2016: 92f), therefore, distinguish between an 'active' and a 'passive' perspective on acceptance. Whereas in the first case a product or measure is positively assessed and approved without reservation by the person concerned, passive perspective taking means to tolerate a measure without worrying or perceiving it as potentially problematic. Moreover, an authoritative strategy of enforced compliance towards measures that one cannot evade is also conceivable, as to be seen in the fields of operational or airport security for example. Being employed in a particular working environment or traveling on

board an aircraft is possible only if one agrees and submits to the intended security procedures—no matter whether they are welcomed or refused.

Explicitly following up on Max Weber's definition of power, Lucke (1995: 104) defines acceptance as the chance to meet the specific or tacit approval for dedicated opinions, measures, proposals or decisions among an identifiable group of people by expecting their acquiescence with good prospects under assignable conditions. The sociological perspective on acceptance is based on an understanding, which regards acceptance as social negotiation processes that are depending on specific perceptions and that are always revisable. In the first instance, acceptance can thus be regarded as time dependent and modifiable. Correspondingly, Bonß (2015: 201) argues that acceptance is always embedded into a sociocultural context and considering these contextual conditions is demanded when decoding the underlying terms of acceptance. In democratic societies, acceptance is of importance due to its mutual dependency with the legitimation of decisions (Lucke 2010) and thus for the legitimacy of security and control measures. Denial of acceptance often functions as more than just an indication of reserved attitudes towards SOSTs. It is rather an indication of reserved attitudes towards the stakeholders that introduce SOSTs to the public. Attitudes towards technology and attitudes towards commercial enterprises or (political) institutions are strongly connected, since institutions often hold responsible for the safe operation of that technology. Thus, "good governance"—characterized by trustworthiness and legitimated decision processes—is an important influential for technology acceptance (acatech-Deutsche Akademie der Technikwissenschaften 2011).

According to Suchman (1995: 574), "legitimacy is a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions". Legitimization strategies thus refer to rhetorical or discursive means for the constitution of legitimacy. The means may differ as the source of legitimacy may vary (e.g., laws, morals, norms, values, interests, etc.) as well as the point of reference of legitimization may be different (e.g., purposes, means, goals). Legitimacy and acceptance are interconnected and decisively interdependent as the former is a precondition for the latter. To this end, various stakeholders and institutions, holding diverse interests, resort on different strategies to gain legitimacy for their decisions. In this regard, Suchman (1995) points to the need for managing legitimacy. Legitimacy management can thus be subject to research to analyze the topoi and argumentation patterns used. As a consequence of Suchman's ideas, it becomes clear that legitimacy is not a phenomenon established once and for all, but consistently has to be renewed and re-established in the lights of historically, politically and socially changing circumstances and contexts that shape the demands for and fabrications of legitimacy.

One of the most prominent concepts on issues of legitimization of surveillance technology is securitization theory. Speech acts of intersubjectively constructing an existential threat to a valued referent object and, based on this, calling for urgent and extraordinary measures to deal with the threat have been analyzed as processes of securitization (Buzan and Wæver 2003: 491). As Balzacq (2011: 1) emphasizes, not the singular speech act is in focus, but the process of negotiation between a speaker

and his audience. This puts the situational—temporal and spatial—context of securitization at center, in which "security articulations" (Stritzel 2007: 370) and actions of the actors are embedded. Fischer et al. (2014) have shown that the perception of security and corresponding security measures arises from particular occasions that generally mobilize for action. However, different countries show varying dynamics of securitization which are influenced by country-specific justification narratives. Putting this indication in the words of Berger and Luckmann (1966), securitization describes a process in which threats are socially constructed. Insofar, shared definitions of social reality come to "acquire the moral and ontological status of taken-for-granted-facts which, in turn, shape future interactions and negotiations" (Barley and Tolbert 1997: 99), they follow a process of institutionalization. To this end, securitization theory is quite close to organizational sociology, describing the dynamics in which institutions are produced or reproduced (Scott 1987). Institutions are predominantly constituted via linguistic processes that define the common understandings of social reality. Phillips, Lawrence and Hardy (2004) describe a model of institutionalization that highlights the role of discourse in processes of institutionalization. The authors describe how discourses make certain ways of thinking and acting possible while others impossible or costly. This way, institutions reinforce their vested interests. They delimit the range of legitimate and illegitimate behavior their members are able to perform without being outlawed among other members of the institution. In this regard, Fairclough (1995: 38) hints at the relevance of a set of rhetorics, which institutions use to facilitate and constrain the social actions of their members:

> "A social institution is an apparatus of verbal interaction or an "order of discourse" [···] Each institution has its own set of speech events, its own differentiated settings and scenes, its cast of participants, and its own norms for their combination." (Fairclough 1995: 38).

Fairclough refers to the shared social values and practices that exhibit how institutions anticipate the social reality of their members. These visions of the institution encompass a whole variety of practices, experiences and perceptions and thus shape the imaginaries of the institutions' members. Assuming issues of surveillance and SOSTs to be subordinate to the same umbrella, perceptions of surveillance and the way they affect other dimensions of social interaction are similarly put into institutional frameworks. These surveillance cultures, i.e., "the ways in which surveillance is conceived and how it relates to other dimensions of social life" (Lyon 2014: 42), constitute and shape the way surveillance is imagined, framed and put into practice.

To summarize, we can say that different rhetorics used to legitimize surveillance become visible by looking at the speech acts of stakeholders in discourses on surveillance and SOSTs. We, therefore, take up the work of Schulze (2015) who identified patterns of surveillance legitimization used by security advocates in the discourse on the so-called "NSA scandal" in Germany. In line with Suchman (1995), Schulze describes the rhetorical strategies politicians utilize to manage the legitimacy of surveillance practices against public scandalization. Denial strategies aim to prevent an escalation by denying that a transgression is already a scandal.

This occurs by denying the existence of a norm transgression or by attacking the scandalizer. Shifting responsibility and delegation strategies occur in later stages when deniability is no longer plausible. This strategy aims to prevent personal damage by framing or blaming other responsible actors. A third legitimization strategy consists in rationalization, likely to occur in middle phases of public contestation. Rationalization strategies are used to increase the personal authority and legitimacy of politicians and other actors involved. Their central aim is to increase the dominance of ideas via presenting them as unquestionable truths. Authorization strategies refer to an authority in charge to state what is right or wrong and what has to be done. Pointing to the singularity of events is a containment strategy that acknowledges the norm transgression but aims at reducing its impact. Finally, Schulze refers to legitimization via emphasizing security issues in processes of securitization. Usually unacceptable norm transgressions gain legitimacy in the face of urgent threats and to tolerate violations of norms and rules which otherwise would have been obeyed.

As these general rhetorical strategies are suitable for various stakeholders in different discourses, they serve as a starting point for analyzing patterns of surveillance legitimization. In addition to the assumption of commonly used strategies to legitimize surveillance in times of scandals, in this contribution we shift the focus towards one particular group of stakeholders in the process of legitimizing surveillance, that is the agents of surveillance legitimization strategies and their institutional embeddedness. Negotiations on surveillance are part of the hierarchical social fabric of dedicated institutional frameworks, in which different stakeholders argue for their vested interests. Via the agents in charge of development or implementation of SOSTs, institutions claim political, economic, organizational or social interests in SOSTs to the individuals affected by surveillance. Being situated in dedicated institutional contexts, the agents resort to institutional rhetorics to call for the legitimacy of surveillance. As addressees of surveillance legitimization strategies, the affected individuals may have the opportunity to assert their acceptance or refusal. The process all too often may not be as linear as depicted. Agents as well as affected individuals have their own interests or may use rhetorics which again impact on the discourse. However, this understanding serves to outline the most relevant elements in terms of the fabrication of surveillance legitimization discourses.

3 Methods

The requirements for the implementation and according exposure to security technologies are often resolved in specialized departments and from there spread among the institutions. In this regard, the responsible employees are in charge to manage the legitimization of surveillance to absorb problems of acceptance in advance and thus to allow for a smooth process of the implementation and use of SOSTs. Professionals of safety and security departments have privileged access to information on decision processes within a given institution. By (pre-)setting intended usage patterns and constructing dedicated problem solutions for SOSTs,

they take responsibility for the implementation and usability of such technologies. As "representatives of an organization or institution" they can be ascribed expert status in the sense of Meuser and Nagel (1991). Holding dedicated responsibilities within a given institutional or organizational context, experts are of interest because of their exclusive experience and body of knowledge regarding a specific setting. According duties, responsibilities and activities are subject to expert interviews. As a person's individual orientations and attitudes embedded in a particular life context may differ from the institutional or organizational setting, they are not subject to the analysis. In contrast, expert interviews aim at elaborating the common body of knowledge, structures of relevance as well as constructions and interpretations of reality within a shared institutional context.

For analyzing institutional rhetorics for legitimizing surveillance, we draw on a set of seven semi-structured expert interviews with safety and security professionals of ENAV, the national air traffic control provider in Italy. The interviews have been conducted as one part of our research activities in the project SAWSOC.[1] SAWSOC aims at achieving convergence between physical and logical security technologies for protecting critical infrastructures. Expert interviews were intended to accompany the technological development in the SAWSOC project by taking into account the demands and expectations of various stakeholders in the project's three use cases. As one of these three use cases, ENAV agreed to arrange interviews with members of their safety and security departments. Whereas the interview guidelines were intended to address potential benefits and negative effects of convergent security systems, feelings of (in-)security and privacy issues, we initially noticed our interviewees engaging in legitimizing the use of numerous SOSTs[2] to protect the critical infrastructure they are operating. Due to the restricted access to internal information about the ATC critical infrastructure, the interviewee sample was compiled via a gatekeeper's selection of interview participants in consideration of the intended research objective. Our sample gathers experts of safety and security departments with various experiences in system engineering, information technology management and/or ATC management. Furthermore, it should be mentioned that initial concerns raised at the beginning of our research regarding systematic errors in sample compilation due to a potential absence of employees with rather skeptical attitudes towards SOSTs did not turn out to be true. Interviews had been conducted in February 2015 during regular office hours at two different locations of the ATC service provider. Conversations lasted for 59:42 min on average and

[1] SAWSOC (Situation AWare Security Operations Center) is a project co-funded under the European Commission's Seventh Framework Program for Security Research. Within the SAWSOC project with its mainly technological outlook, we were responsible for the socio-scientific side of research, focusing on the relationship between security technology and feelings of (in-)security. For further information on SAWSOC see the project's website www.sawsoc.eu.

[2] Surveillance measures to protect the air traffic control critical infrastructure from unauthorized intrusions had been a major topic of the interviews (e.g., mantraps, ID cards and CCTV as well as passwords, firewalls and intrusion detection software). Despite that, interviewees also addressed safety and security issues concerning air traffic control itself. We did not analyze elaborations on the latter, as radio between pilot and ground service, collision warning systems or radar did not fit into our understanding of SOSTs.

afterwards had been transcribed fully verbatim from digital recordings. In total, we compiled 6 h 58 m of interview material.

We used qualitative content analysis to identify underlying patterns of argumentation as a rule and theory guided and thus methodological-controlled approach for analyzing verbal data that allow for inter-subjective verification of interpretations (Mayring 2000). The analysis aims at developing a system of categories and corresponding text segments which serve to either sharpen the focus or appear to be relevant for the examination with regards to content. We, therefore, use a hybrid of deductive–inductive construction of categories (Kuckartz 2012: 69): the main categories as identified by Schulze (2015) are a starting point for our analysis. A check of their fit for the intended research question and according constructions of subcategories is then carried out inductively proximate to the interview material. This way the system of categories develops in an iterative process. For each interview segment that fits the criteria of one of the existing categories a decision is made whether or not to subsume to a coded segment under an existing category or if the preliminary system of categories needs to be extended in the sense of inductive categorization. Organizational and technical issues of SOSTs are disregarded in the process of coding as far as they are not of relevance for an increased understanding of the research question. Data analysis conducted was computer assisted using MAXQDA. In total, we assigned 40 codes with an amount of 237 codings. In the following section, the retrieved system of categories is interpreted bearing in mind the underlying research question. In line with the convention by Kuckartz's (2012), interviewee citations are documented as such and visually separated from the analytical conclusion of the authors.

4 Analysis

Although not being on our initial agenda, we noticed some of our interviewees having a dedicated need to justify the development and implementation of new SOSTs within their institution. During the process of qualitative content analysis, it soon became clear that some of the different rhetorical strategies utilized to legitimize surveillance are pronounced more incisively and to the point compared to others. In addition, certain expressions are used more frequently than others and appear to be in the center of one coherent rhetoric. The following sections present all of the legitimization strategies identified and give a brief description accompanied by illustrative examples for their usage. "Section 4.1" summarizes those rhetorical strategies that were used less frequently. "Section 4.2" introduces the more prominently used rhetorics that form a basis for identifying what can be called an institutional security culture for legitimizing surveillance.

4.1 Denial, Rationalization, Delegation, and Singularity

4.1.1 Denial

A basic strategy for legitimizing a behavior is the denial of (possible) problems. These strategies, coded as denying a scandal/problem in our material, show up, e.g., when a respondent was asked about negative effects of convergent security systems:

> Potential negative effects. No. I think, as I said, it's a goal, it's a target for us to have a convergence between this two part of security. (Interviewee 5).

Negative effects are directly denied and convergent SOSTs are described as positive and an aim to achieve. Despite this very banal variants, there are also versions (sometimes embedded within other legitimization strategies), which implicitly acknowledge the possibilities that some people could have problems with such technologies, but still those problems are brushed aside and denied. In this context we could identify the subcode deny knowledge/evading the issue, which can particularly be found as a reaction to critical questions, e.g., about privacy issues. Characteristic for those are stuttering, avoiding a clear answer and or/admitting ignorance:

> Privacy··· [longer pause]. Ok, starting from the point that availability, integrity are the must for [our company], also confidentiality of information is important. And privacy about the people's live, the people's personal data··· [longer pause] I don't know very well. I am sorry about that. (Interviewee 7).

Even if there is no stuttering, some other examples show variants of this strategy, where the critical question is just not answered. A question, which describes the issue that convergent security control rooms remind some people of a total surveillance like the novel 1984 by George Orwell depicts, is picked up by one of the respondents; however, the actual answer revolves around the resilience of such control rooms. The critical issue about privacy is avoided.

Another subcode found is called rebranding. Beyond the primary definition of changing the denomination of SOSTs, we could find examples where the issues arising from surveillance technologies are rebranded. Both variants are found quite rarely in our sample, showing up as one example where control and surveillance functionalities of mantraps are downplayed by positively referring to them as "security checks". Similarly privacy issues of SOSTs are rendered as unimportant complaints by calling them "blah blah blah".

One can see that strategies in this main code are often found as a reaction to questions about privacy, which especially leads to avoidance. However, some answers seem to be a plain claim that SOSTs are generally not problematic, do not lead to problematic issues or that at least the respondents have no knowledge about such issues. Despite such denial strategies, the same respondents also used other legitimization strategies during their interviews and thus apparently still had the urge to justify the usage of SOSTs.

4.1.2 Rationalization

The general aim of strategies which fall under the category of rationalization is to present an action or idea as well-thought-out and thus reasonable. One way to achieve such a result is to declare facts. Facts are statements which are presented as "objective" and do not need further clarifications, while at the same time a need for surveillance is implied. As an answer to the question why it is all right that only a few people working in the security operations centre (SOC) have control of all the data of a company, one answer is simply that someone has to know all about the company. A similar example, also in response to privacy questions, is the statement:

> Privacy is not a friend of [laughs] safety and security. (Interviewee 5).

No further explanation is given for such a statement; it is merely presented as a fact. The humorous manner in which the above example is presented underlines the implicit superiority of security necessity over privacy issues present in such statements.

Another possible strategy to support the rationality of an action is to present it as normal. Some examples of this normalization strategy can be found in our interviews, when comparisons to the use of surveillance technology in other countries or institutions are made. Also found in this code is a statement, which pronounces the ubiquity of SOSTs at the workplace and the habituation which comes along with this, thus normalizing them. However, those strategies are quite rare in our material and are mostly not in the focus of an argument. One interviewee explicitly put emphasis on technological innovations in IT which naturally comes along with enhanced and extended data collections in many areas.

Strategies with the main focus on the rational appeal of the argument or the stated action is not a strongly pronounced feature we could identify. This does not mean that other legitimization strategies are not presented as rational. However, focusing primarily on phrasing arguments in a way to appear thoughtful and intelligent, and implying the conclusion that SOSTs are necessary though, is only found in very few examples and as such the entire code of rationalization is one of our least coded categories.

4.1.3 Delegation

Although we found four different subcodes within the main code, delegation is a relatively minor aspect within the legitimization strategies of our respondents. There are still some examples obtained from the material. Two quite similar subcodes which could be found are shifting to experts and shifting to superiors.

'Shifting to experts' shows a certain similarity with the code of expert authority, but differs in its logic. Examples within this subcode are primarily concerned with shifting the responsibility for SOSTs and related issues to experts and implying that the respondent is not the one to ask about whether or not there are issues. Arguments that fall under the expert authority code also try to shift the responsibility to some degree, but the focus of the argument is that only experts know what has to be done and all the others have to follow this authority and accept it as legitimate. The code

shifting to superiors is very clear in its pattern. Arguments within this code state that a superior institution or stakeholder ordered to invest in security and address security issues. Problems or negative effects become their responsibility and the decision to do it is presented as out of reach of those who are tasked with it.

Another identifiable subcode in this category is called trust. This is used for examples where surveillance technologies are presented as acceptable, because the ones who maintain those are deemed trustworthy:

> I would like to know what they do with my data. Even though I trust that they do the right thing, but I would like to know, of course. (Interviewee 5).

Although the desire is expressed to know what exactly the data are used for, the respondent inherently trusts the company. Another example shows more clearly how this functions as a legitimization. When asked about privacy issues regarding biometrics, one answer is that as long the data are correctly managed by the company, it is deemed unproblematic, even though it is possible to know where a person is at any given time. Trust in the well functioning of the system seems to be enough to accept SOSTs. By trusting others to maintain the security in a way that is deemed unproblematic, the responsibility to question, consider and integrate SOSTs and possible unintended side effects is delegated to those who are in charge of the operation and maintenance of the system.

Finally, there is one legitimization pattern which differs slightly from the ones mentioned before. While in other arguments responsibility is generally shifted to third parties, the subcode sharing responsibility describes examples where the accountability for the proper implementation and maintenance of SOSTS is partly accepted. Nevertheless, at the same time it is also referred to the responsibilities of other actors.

4.1.4 Singularity

Legitimization strategies under the main code of singularity stress the limited nature and scope of surveillance or security technologies. In our material, we found two specifications of singularity, differing in the argumentation in which way the surveillance appears limited. The first one is limited purpose. A recurring theme which is present in our interviews is that a difference is made between a surveillance due to security reasons and a surveillance due to control reasons. It is emphasized that surveillance technologies actually can track people within a facility, but that tracking is not used to control the working hours of the employees, which is seemingly deemed not acceptable. In reverse, surveillance technologies are interpreted as acceptable as long as they are used for security reasons only and not to control the commitment and performance of employees.

In addition, we found strategies that emphasize the limited spatial character of surveillance measures (limited spatial dimension). If monitoring is restricted to the workplace, surveillance is not considered as a problem. Respondents state that the surveillance is only work related, and as far as they are only there to work, there is no issue with it. Moreover, as an answer to the question why security checks in the company are necessary, one can find another variant of this code, which states the

company the respondent works for is a very specific environment with a lot of critical assets. In such an organization, extensive surveillance is deemed necessary and acceptable, confining the legitimacy of surveillance to this specific locality. Especially this last argumentation, but actually the whole main code of singularity, shows obvious links with a lot of the other legitimization patterns found. Many of them are implicitly or explicitly connected to the working place of the respondents.

4.2 Authorization, Securitization, and Pragmatism

4.2.1 Authorization

The main code of authorization is the one for which we could identify the most examples and as such stands at the beginning of this segment about the most frequently used strategies found in our material. In this regard, the most prominent subcode is the one we called experts versus laymen. Within this subcode one finds examples, where a discrepancy of the knowledge about security issues between experts and other people is stated. The general argument is that the experts know what they are doing and thus the implementation and usage of surveillance technology is not a problem per se, even if the laypeople do not acknowledge this at the moment. This subcode of experts versus laymen can be further differentiated into subcodes which highlight specific aspects of legitimizations in this vein.

A very common and important sub-strategy is one we called teaching and education. Summarized in this code are legitimizations which focus on the idea that employees have to be trained and educated to share the vision of the company and/or to build awareness about security-related issues. This is in line with the upper level code of experts versus laymen, but puts the focus on the element that those experts have to teach the laymen about surveillance, security technology and procedures. The legitimizing aspect of those arguments are found in a sometimes explicit, sometimes implicit logic that if one is able to educate the unknowing employees, those will realize that surveillance cameras or similar technologies are only used to ensure security, and thus are necessary and in no way problematic. Both legitimation strategies draw a hierarchy between experts and laymen where the former has to educate the latter, since the experts know what is right to do whereas the others are more or less ingenuous concerning security questions.

Two other subcodes in this area focus even more on fortifying the expertise of some people in contrast to others; these are personal authority and expert authority. Both strategies function in a comparable way, but with the difference that either the own authority or the authority of certain experts is stressed. Personal authority is evoked when, e.g., opinions about convergent security solutions are described as positive with the addendum that the respondent has worked in the field of security before and thus is experienced in this matter. Other examples focus on the fact that it is the respondent's job to ensure security and insofar he or she has the authority to use the technology which is deemed necessary. Expert authority is a similar strategy, but it is not the speaker who is presented as authorized and knowledgeable to decide about the usage of SOSTs, but some experts. Apart from that, we can localize this strategy in the context of privacy questions, as we found arguments

which state that there are experts which are reliable and thus are authorized to make decisions in this regard.

Beyond the subcode experts versus laymen and its differentiation, the main category authorization also includes another subcode with numerous codings: impersonal authority. This includes statements which refer to a legal and/or institutional regulation which authorizes and regulates the operation of surveillance technologies, thus producing a sense of legality and acceptance. On the one hand, laws or institutional policies and rules are considered to solve problems emerging from surveillance like the privacy of data, as data protection is regulated by law which is usually regarded as legitimate. On the other hand, laws and policies are also used to legitimize the usage and implementation of SOSTs, as they state what technology has to be used and that those concerned with security shall follow those rules. Our examples show the pattern that if SOSTs are managed within the borders of a particular law or policy which is considered legitimate, SOSTs themselves cannot be illegitimate.

A minor subcode of authorization, which nevertheless could be identified for a few examples, can be called role model. The examples found in our interview state that there are practices comparable to some security measures in other fields, domains or areas (e.g., safety regulations) which are adaptable for security solutions, implying if it is.

4.2.2 Securitization

During our research, we have identified numerous arguments that fall under the main code of securitization. Here, we include statements that argue for a need for security to protect something or somebody from a defined threat. In our material, the perception of threats can be conceptualized and divided into the subcodes existential threats and new or unknown threats.

Both subcodes have a lot in common, but the nature of the threat is different. Legitimizations based on existential threats focus on the life-threatening nature of dangers and the necessity for security solutions, since the life of people or, as it is explicitly said by one respondent, the national security depends on that. Distinctive for our case are statements which declare such a necessity due to threats which are new or unknown. New threats are often envisioned to be connected to new technologies. Often a need to protect the own data against attacks from the web is stated. Additionally, a perceived increase of international terrorism is also mentioned as a new threat, which again implies a necessity to react with an increase of SOSTs. The important aspect is that those threats are new and the security technology has to adapt to these. New and suitable systems are needed, whereas the aforementioned existential threats are already seen as a reality which, due to its grave importance, needs more security solutions than other areas. Accordingly, it is legitimate to have a comparatively high level of implemented SOSTs in the ATC sector, as it faces such existential threats.

Apart from this, there are patterns which focus more on giving reasons or explaining how and why it is necessary to secure certain premises against threats instead of describing those threats. Legitimization through altruism is such a

strategy which argues that SOSTs serve a certain group of people and that security measures are implemented to benefit people who expect a particularly high level of surveillance. It is also used to declare that security technology helps affected people to feel more secure and thus results in a positive effect. The last subcode under this topic we could identify is named (pseudo) causality. Here, a causality is constructed, where missing actions lead to negative consequences. Examples predominantly describe chains of causations which could happen if the premises of the company in question are not extensively protected by security measures.

4.2.3 Pragmatism

In addition to our initial framework of codes, we could identify a number of legitimization strategies which cannot be subsumed under the ones before, but form a coherent logic. For those, we formed the main code of *pragmatism*. What we mean by that is a very practical work-oriented approach presented by the respondents which reveals an inherent acceptance—and thus legitimacy of surveillance technology—and avoids complex or comprehensive justifications.

In general, speech acts in this manner were quite common in our material, which we divided into four subcodes. Beginning with two less frequent ones, we could identify patterns which we subsumed under the codes financial compensation and nothing to hide. The few examples are, nevertheless, quite distinctive in their argumentation. They are reactions to questions about problems or discomfort with surveillance at the workplace on the part of the respondents. One argumentation focuses on the financial aspect: an employee is getting paid for the work and that seems to compensate possible discomfort. The other subcode focuses on a kind of naiveté: as long as one has nothing to hide, e.g., illegal activities, one should not have a problem with exposing ones data.

More frequent is a legitimization strategy, which we subsumed under the subcode efficiency. This is reserved for examples, where a notion can be identified that more or new surveillance technology is simply more efficient and thus better suited to provide the necessary security. This strategy is commonly used when questions concern convergent security systems. The argument usually stresses the idea that such systems would improve security, so they are presented as a good idea to implement and expand them, again taking a very practical approach in this matter. New or more efficient technology is simply presented as better suited to achieve the goal of ensuring security. So it seems to be legitimate and reasonable to use them.

The most frequent subcode and a very noteworthy one for our following discussion is the one we called *rules of the game*:

> Yes we have to release personal details and you have to consider it as manage in the right way according to our internal policy. Then we can't prevent people in having different perceptions of it, so someone could consider it as a disturb, even as something is going to let's say jeopardize their individual rights. But I mean you have been recruited, selected to do something, you were accepting the rules of the game entering our agency. [···] That's life. (Interviewee 3).

This subcode is named after this idea present in the example above. It becomes clear that the respondent is of the opinion that privacy infringement and surveillance comes with the territory or as it is said, is just part of the game, the game being air traffic control. Part of this argument is the knowledge about this. If you are going to work in such an environment, you know that surveillance takes place, thus one has no reason to complain about it afterwards. Other examples for this subcode show a slightly different layer of the legitimization pattern, which depicts something like a barter: being under surveillance is necessary to ensure security. Thus, one has to accept it and give up some of the personal freedom to achieve this goal. Again this is presented as something one knows and has to live with in such an environment. In general, these legitimization strategies are reactions to questions about privacy infringement. They constitute a pragmatic logic that the people are doing their job in a certain kind of setting, which demands certain security measures. They have to accept these requirements, even if it means privacy infringement to a certain degree, since it is all part of the game.

4.3 Relations Between Different Legitimization Strategies

Table 1 shows the relative frequencies of codings as identified in Schulze's (2015) analysis of strategies for surveillance legitimization used by politicians in comparison to the rhetorical strategies used by experts of safety and security departments at an ATC critical infrastructure in our analysis. Frequencies in bold letters indicate those rhetorics used most prominently, frequencies in italics indicate comparatively prominent rhetorics.

Amongst politicians, denying and authoritative strategies are most prominently expressed and are accompanied by rationalizations and speech acts of delegation. Experts of ATC safety and security more often rely on authorization and securitization strategies or refer to pragmatic aspects to legitimize surveillance. Although—due to content-related differences in codings—not a systematic comparison, Table 1 supports the assumption that different stakeholders in discourses on surveillance legitimacy rely on dedicated strategies due to their institutional embeddedness.

Table 1 Relative frequencies of codings

Strategy	ATC experts (present study) (%)	Politicians (Schulze 2015) (%)
Denial	10	23
Rationalization	8	17
Authorization	28	21
Securitization	21	11
Pragmatism	15	–
Delegation	9	16
Singularity	9	12
Sum	100	100

Comparing the most prominent rhetorical strategies, it becomes apparent that they form a cohesive pattern of reasoning. The position of politicians calls for an approach to legitimize surveillance more frequently by disputes, using authoritative and denying rhetorics. The own integrity is meant to be protected by delegating responsibilities or arguing in the rational-legal sense of bureaucratically elected sovereign. As a reaction to the very needs of a bureaucratic institution, ATC safety and security experts tend to focus on three main aspects:

1. The air traffic domain is a specialized branch, facing dedicated and—according to our interviewees—new and/or existential threats (Securitization).
2. Within this branch, one finds knowledgeable experts being aware of these threats and having the authority to implement means to ensure security and thus "educate" the unaware (Authorization).
3. This aspect must be tolerated when being employed at an ATC critical infrastructure, in which institutional needs are prioritized before privacy concerns (Pragmatism).

This line of arguing sets up an environment where privacy issues, as the one problem of SOSTs most commonly referred to, are subordinate to the provision of security. Additionally, even the more uncommonly used legitimization strategies often fit into the pattern. Singularity arguments show an emphasis on locality, thus connecting the use of SOSTs to this specific work environment. For rationalization and denial, we find strategies of normalization and the evading or denial of problems, also adding to the idea that SOSTs are an integral part of the ATC branch and remaining potential problems are sometimes not even addressed. This overarching rhetoric and also especially the legitimization strategies coded as rules of the game lead to the understanding that the institutions' vested interests facilitate and constrain their members' ways of thinking and talking about surveillance and security. However, the following statement of one interviewee hints towards potential variations according to occupational position differences within one and the same institution:

> On the other side taking on board only my answer you might have the management view, which might completely differ from let's say frontline operator view or if you go interviewing a trade union representative [···] but I mean that is part of the game again (Interviewee 3).

The important aspect is an understanding of different stakeholders having a specific way of thinking and arguing about security. In addition, the last sentence of the quotation suggest that the "rules of the game" do not only urge one to accept SOSTs but, moreover, to accept a vision of security engrained in the institution that enables and suggests a specific way of thinking, talking and handling security measures. In this sense, our expert interviews shed light on this common body of knowledge about surveillance and security technologies which is shared among the stakeholders of an institutional security culture, shaping specific rhetorics and leading to the use of particular legitimization strategies.

5 Discussion

Institutions delimit the range of actions their members are able to perform. Negotiations on the legitimacy and illegitimacy of actions make certain ways of thinking more costly compared to others and this way reinforce the shared social values and practices that exhibit how institutions set a social reality for their members. In others words, they establish a dedicated institutional culture by structuring practices with and perceptions of different realms of experience. Discourse is one prominent element in this process of institutionalization.

In this article, we identified a comprehensive set of rhetorical strategies used by experts of safety and security departments to legitimize surveillance and the use of SOSTs in the context of an air traffic control critical infrastructure. We found these patterns of surveillance legitimization to be embedded in a specific institutional environment, in which the way of conceiving surveillance, putting it into practice and assessing its outcomes is highly determined. Negotiations on the legitimacy of surveillance practices do not take part in discourses free of hierarchies. They are rather part of one institutional surveillance culture (Lyon 2014: 42), in which reference to a set of selected rhetorics is more likely compared to others. The experts of safety and security departments of an ATC critical infrastructure in our sample most prominently featured the main rhetorics of authorization, securitization and pragmatism. These recurring themes form a coherent line of argumentation, in which the legitimization strategies of our interviewees revolve around the threats they are facing in the air traffic domain. This is also used to explain why privacy infringement is a necessity and normality in this domain to be tolerated when working in this branch. Experts of safety and security departments, moreover, are in charge of educating other employees. Reference to these most pronounced legitimization patterns signifies a rhetoric that focuses on constructing the air traffic domain as a specialized context in which SOSTs are a common necessity. As Fairclough noted,

> "It is [···] necessary to see the institution as simultaneously facilitating and constraining the social action of its members: it provides them with a frame for action, without which they could not act, but it thereby constrains them to act within that frame." (Fairclough 1995: 38).

Comparing our findings with Schulze's (2015) analysis of politicians' rhetorical strategies to legitimize surveillance, we see clear differences between the two different types of stakeholders. Whereas politicians utilize selected rhetorical strategies suitable to highlight their sovereignty as rational authorities, ATC experts rely on discursive actions in line with their company's pragmatic way of handling issues of security, surveillance and privacy and thus reinforce—in the words of an interviewee—"the rules of the game".

The previous sections do not claim to systematically or comprehensively summarize the difficulties that arise in analyzing negotiations of surveillance and the use of SOSTs. A comparative analysis of the institutional conditionality of rhetorics for legitimizing surveillance needs a more systematic contrapositioning of

discoursive actions to be identified within different institutions. Furthermore, it is not our intention to present our interviewees as uncritical in terms of their attitudes towards surveillance and SOSTs. Our interviewees may accept and reproduce an institutional security culture in their legitimization rhetoric, but they are also reflexive on contradictory aspects. We did find several examples where critical aspects of SOSTs are mentioned and ambivalent opinions on these topics are surfaced. In the perspective of most of our interviewees, technology is not considered as a universal remedy for the prevention of intrusions. We, therefore, like to acknowledge the presence of ambivalent attitudes towards surveillance, as some interviewees on the one hand reproduce the institutional security culture, but on the other hand also reflect on it while de-constructing legitimizations. However, the comparison of different patterns of surveillance legitimization and their institutional embeddedness as proposed in this article provides an important step towards an evidence-based discussion of the institutional conditionality of negotiations on surveillance issues and the use of SOSTs.

The explorative approach presented in this article may serve as a starting point for further investigations. Extending the data to include agents from various domains seems a necessary next step to allow for a more systematic comparison. Additionally, a historical perspective could be beneficial to gain further insight into how changing institutional contexts impact on legitimization strategies. Picking up the observations of Bigo et al. (2014) outlined in the introduction, our findings support the assumption that the policy-making process on surveillance and security still sidesteps a number of societal actors. The fact, that the biggest group of stakeholders, the citizens, appears to have the least influence in the decision making process on the factual arrangement of security technologies and according surveillance practices is a serious challenge. Especially in democratic societies, the legitimacy of personal civil rights and privacy intruding security measures can become contradictory, as they are reinforced by the very needs of a bureaucratic institution.

References

Acatech–Deutsche Akademie der Technikwissenschaften (2011) Akzeptanz von Technik und Infrastrukturen. Springer, Anmerkungen zu einem aktuellen gesellschaftlichen Problem. Berlin and Heidelberg

Balzacq T (2011) A theory of securitization. origins, core assumptions and variants. In: Balzacq T (eds) Securitization theory. How security problems emerge and dissolve, 1–30. London: Routledge

Barley SR, Tolbert PS (1997) Institutionalization and structuration: studying the links between action and institution. Organization Stud 18(1):93–117

Berger P, Luckmann T (1966) The social construction of reality: A treatise in the sociology of knowledge. Penguin Books, London

Bigo D, Jeandesboz J, Martin-Maze M, Ragazzi F (2014) Review of security measures in the 7th research framework programme Fp7 2007–2013. Edited by Justice et Affaires Intérieures (LIBE) Commission des Libertés Civiles. Brussels: European Parlament

Bonß W (2015) Akzeptanzprobleme und die normative Kraft des Faktischen. In: Zoche P, Kaufmann S, Arnold H (eds) Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung, 199–218. Münster: Lit

Bonß W, Wagner K (2016) Sicherheitspositionen. Zur Perzeption und Diskussion von Sicherheitsmaßnahmen am Flughafen. In: Masala C, Fischer S (eds) Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? 85–101. Wiesbaden: Springer VS

Buzan B, Wæver O (2003) Regions and powers: the structure of international security. Cambridge University Press, Cambridge

Degli Esposito S, Santiago Gómez E (2015) Acceptable surveillance-oriented security technologies: insights from the SurPRISE project. Surveill Soc 13(3/4):437–454

European Commission (2006) FP7—Tomorrow's answers start today. European Commission, Community Research. Online: https://ec.europa.eu/research/fp7/pdf/fp7-factsheets_en.pdf. Accessed 26 July 2016

European Commission (2012) Security industrial policy: Action plan for an innovative and competitive security industry. COM(2012) 417 final. Brussels: European Commission

Fairclough N (1995) Critical discourse analysis: The critical study of language. Longman, London

Fischer S, Klüfers P, Masala C, Wagner K (2014) (Un-)Sicherheitswahrnehmung und Sicherheitsmaßnahmen im internationalen Vergleich. Forschungsforum Öffentliche Sicherheit (Schriftenreihe Sicherheit Nr, Berlin, p 14

Kuckartz U (2012) Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung. Weinheim: Beltz Juventa

Lucke D (1995) Akzeptanz. Legitimität in der Abstimmungsgesellschaft. Opladen: Leske + Budrich

Lucke D (2010) Akzeptanz und Legitimation. In: Kopp J, Schäfers B (eds) Grundbegriffe der Soziologie. Leske + Budrich, Opladen, pp 12–17

Lyon D (2014) Situating surveillance: history, technology and culture. In: Boersma K, van Brakel R, Fonio C, Wagenaar P (eds) Histories of state surveillance in Europe and beyond, 32–45. New York: Routlege. Online: "https://cryptome.org/2014/06/histories-state-spying-eu-plus.pdf". Accessed 22 Aug 2016

Marx GT (2002) What's new about the "new surveillance"? Classifying for change and continuity. Surveill Soc 1(1):9–29

Mayring P (2000) Qualitative content analysis. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research 1(2). Online: http://nbn-resolving.de/urn:nbn:de:0114-fqs0002204. Accessed 26 July 2016

Meuser M, Nagel U (1991) ExpertInneninterviews—vielfach erprobt, wenig bedacht: ein Beitrag zur qualitativen Methodendiskussion. In: Bogner A, Littig B, Menz W (eds) Das Experteninterview: Theorie, Methode, Anwendung, 71–93. Opladen: Leske + Budrich

Pavone V, Degli Esposito S (2012) Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. Public Understanding Sci 21(5):556–572

Phillips N, Lawrence TB, Hardy C (2004) Discourse and institutions. Acad Manag Rev 29(4):635–652

Renn O (2005) Technikakzeptanz. Lehren und Rückschlüsse der Akzeptanzforschung für die Bewältigung des technischen Wandels."*Technikfolgenabschätzung* 14(3):29–37

Schulze M (2015) Patterns of surveillance legitimization: the german discourse on the nsa scandal. Surveill Soc 13(2):197–217

Scott WR (1987) The adolescence of institutional theory. Adm Sci Q 32(4):493–511

Stritzel H (2007) Towards a theory of securitization. Eur J Int Rel 13(3):357–383

Suchman MC (1995) Managing legitimacy: strategic and institutional approaches. Acad Manag Rev 20(3):571–610