Ochs, Carsten; Pittroff, Fabian; Büttner, Barbara; Lamla, Jörn

Article

Governing the internet in the privacy arena

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Ochs, Carsten; Pittroff, Fabian; Büttner, Barbara; Lamla, Jörn (2016) : Governing the internet in the privacy arena, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 5, Iss. 3, pp. 1-13, https://doi.org/10.14763/2016.3.426

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 3

Governing the internet in the privacy arena

Carsten Ochs
Department of Sociological Theory, Universität Kassel, Germany, carsten.ochs@uni-kassel.de

Fabian Pittroff
Department of Sociological Theory, Universität Kassel, Germany, pittroff@uni-kassel.de

Barbara Büttner
Department of Sociological Theory, Universität Kassel, Germany, barbara.buettner@uni-kassel.de

Jörn Lamla
Department of Sociological Theory, Universität Kassel, Germany, lamla@uni-kassel.de

Published on 30 Sep 2016 | DOI: 10.14763/2016.3.426

Abstract: The surveillance disclosures triggered by Snowden have fueled the public re-negotiation of privacy. To follow resulting controversies we present a methodology that links social worlds theory to approaches asking for the democratic governance character of issue-centred arenas. After having outlined this approach it is put to the test. We analyse and compare two cases: the Schengen/National Routing, and the Parliamentary Committee investigating the NSA surveillance disclosures. The analysis reveals two oscillating governance modes at work in the privacy arena; their interplay results in an obstruction. Based on this observation we finally provide a diagnosis of possible future arena trajectories.

Keywords: Privacy, Democracy, Digitisation, Arena Methodology

Article information

Received: 25 Apr 2016 **Reviewed:** 17 Jun 2016 **Published:** 30 Sep 2016

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/governing-internet-privacy-arena

Citation: Ochs, C. & Pittroff, F. & Büttner, B. & Lamla, J. (2016). Governing the internet in the privacy arena. *Internet Policy Review*, *5*(3). DOI: 10.14763/2016.3.426

This paper is part of Doing internet governance, a special issue of Internet Policy Review *guest-edited by Dmitry Epstein, Christian Katzenbach, and Francesca Musiani.*

INTRODUCTION

For quite a while now the spread of digital networking practices fuels discourses that render problematic the way privacy is destabilised by informational means (e.g. Schaar, 2009). The global surveillance disclosures triggered by Edward Snowden in 2013 and the involvement of prominent political actors (e.g., Merkel, Rousseff) and institutions (e.g., intelligence services, governments) have further boosted these discourses and the public re-negotiation of privacy. In this article we will deal with these controversial processes. Taking the 2013 disclosures as a starting point from where to follow the controversy (Pinch & Leuenberger, 2006) we focus on the "Struggles and Negotiations to Define What is Problematic and What is Not" (Callon, 1980). We hold that in answer to Snowden's revelations numerous social worlds began to publicly specify problem definitions, and to propose solutions accordingly; some of the problem/solution packages were incommensurate and some were compatible, but all of them constituted what we call in the style of Anselm Strauss (1978) and Adele Clarke (1991) the *privacy arena*: the virtual place where social worlds gather to argue and struggle around privacy, i.e., where they define the initial situation and the actors involved, specify the problem, and put forward diverse solutions.

Before specifying this approach in detail (1) we would like to point out that by focusing on controversies we take up a radically *agnostic* stance (Callon, 1986) towards privacy: we will completely abstain from specifying any *a priori* understanding of the concept and its normative weight. We know very well that such specifications fill enormous bookshelves, and elsewhere we have contributed to further filling them (e.g., Ochs & Ilyes, 2014; Büttner et al., 2016). Yet, here we will bracket our knowledge and focus exclusively on segments of the public renegotiation of privacy that emerged in answer to the surveillance disclosures. We will analyse two such segments: the Schengen/National Routing (SNR) proposal (2) and the German Parliamentary Committee investigating the NSA surveillance disclosures *(NSA-Untersuchungsausschuss)* (3). As will be explained, in the negotiations encountered in these segments privacy is generally set in relation to a whole web of values, interests, routines, distinctions etc. In this sense, what is at issue in the controversies is the sociotechnical set-up and governance of the internet at large. As our analysis reveals there are two oscillating governance styles to be identified in the privacy arena (as far as we have investigated), i.e. two ways of (more or less democratically) dealing with the issue. Their interplay results in an obstruction of the democratic search for appropriate problem definitions and according solutions. We will finally summarise and provide an analytic diagnosis concerning possible paths future developments within the privacy arena may take if the blockade remains (4).

SECTION 1: METHODOLOGICAL PRELIMINARIES

Our ultimate interest as pursued in this article is to prove the validity of our methodology for studying the public renegotiations of privacy as processes pertaining to "technical democracy" (Callon, Lascoumes, & Barthe, 2011). Having said this, our goal is to flesh out a framework that a) allows to *follow the controversies and renegotiations concerning privacy*, and b) to *analyse the democratic style of these struggles*.

To do so, we take up a classic science and technology studies (STS) approach, namely the "Theory/Methods Package" (Clarke & Leigh Star, 2008) provided by social worlds/arenas theory. The latter goes back to Anselm Strauss who holds that contemporary social formations

consist of a multitude of social worlds. These worlds are constituted by specific core activities differentiating a social world from the rest of the world; core activities are in turn based on material-symbolic techniques carried out by human organisms and their material contemporaries, and they unfold at (perhaps virtual) places (Strauss, 1978: 122). Thus, a social world is characterised by what is done there (core activity), how it is done (technique), and where it is done (place). In the course of establishing and stabilising a social world some type of organisation may emerge and processes of authentication and legitimation occur: actors negotiate definitions pertaining to the elements and practices making up the given world (Strauss, 1978: 122-126; 1982: 172-173). Thus, insofar as the building blocks of social formations (read: social worlds) are conceived as contested settings from the outset, it is collective processes of negotiating practices and sociotechnical order that are at the very heart of social worlds theory. However, when turning the lens from a single social world towards the wider set-up it is located within, the struggles and negotiations *among* social worlds appear; these constitute *arenas*, i.e. those sites where diverse social worlds gather around specific issues so as to engage in disputes, negotiations and struggles about the legitimate composition of the world, etc. (Strauss, 1993: 225-232).

In the case that interests us here the issue of privacy constitutes an arena where social worlds renegotiate privacy's status. The overall privacy arena is composed of various segments that break down the issue into specific sub-issues and treat the overall issue accordingly. Our research question concerns the democratic character of such negotiations. It is important to note that by using the term "democracy" we do *not* refer to a specific form of institutionalised government nor to political regimes disposing of specific institutional procedures. Instead, we use the term in the sense of John Dewey (1946) to denote *societal learning processes*. These involve the building of issue centered publics and may feature several phases of defining groups and their interests, of building associations, naming experts, determining representatives, of problematising and devising solutions, of trial and error etc. Asking for the democratic character of the negotiations encountered in the privacy arena thus amounts to analysing the political features of the corresponding learning processes in a broader way than pursued in classic political science insofar as the approach that we follow directs attention to public arguments that may or may not involve the conventional institutions of political (democratic) systems. [1]

In what follows we present a "methodological showcase": we will provide brief analyses of two different segments of the privacy arena where specific problematisations/solutions are negotiated. As our ultimate interest lies in showing that the approach promoted here allows for specifying the democratic character of the arena negotiations, we will only go as deep into the case studies as is required to prove the validity of the methodology; and we will restrict the analysis to the minimum number of cases to be compared when following the comparative method (Glaser & Strauss, 1998).

SECTION 2: SCHENGEN/NATIONAL ROUTING (SNR)

The global surveillance disclosures have shown the general public quite plainly the dimensions of the digital crisis of privacy. What are the democratic response patterns emerging in reaction? To tackle this question we successively chose cases promising to feature analytically differing characteristics. [2] As a start, we selected the Schengen/National Routing (SNR) discourse as segment of the privacy arena. The SNR problem/solution package came up as a direct reaction to the Snowden revelations (Dönni, Machado, Tsiaras, & Stiller, 2015). The proposal focuses on routing data packages in a territorially framed way, either within the Schengen area or within

the nation state. Hence, it aims at providing a technical fix (routing) for a social problem (surveillance); we therefore presumed to come across a constellation where the sociotechnical dimension becomes visible easily – a readily analysable STS case.

To see what the SNR proposal results in we have first to understand that the internet as a "network of networks" is composed of so-called “autonomous systems” (AS) [3] run by private or public corporations (e.g. commercial Internet Service Providers (ISPs) or universities). When sending a data file via the internet the file is broken down into a number of data packages (IP packages). Those packages include information concerning their origin and the target address, and they are sent independently from each other (Tiermann & Goldacker, 2015: 14-15). When a file is sent from a device, its constituent IP packages are firstly routed through the AS the device is connected to; at some point the IP package transits into another AS with whom the “original” provider (ISP or public entity) has a peering (big carriers agree to mutually route each other’s traffic), or a transit contract (small providers pay large carriers for routing their IP packages).

Thus, the IP packages composing a file when they travelling through the internet, the IP packages composing a file are likely to pass through a multitude of further AS, and they thereby may take different routes (Dierichs & Pohlmann, 2008): which way a package takes is not predetermined a priori, and there is no central navigation. Instead, packages are sent in stages, from one router to the next. Routing protocols define the way a package is sent on: within AS’ there are so-called *Interior Gateway Protocols* routing the data flow, such as the "Open Shortest Path First" protocol (OSPF); *Exterior Gateway Protocols* govern how data packages are sent on between AS’. When IP packages pass from router to router the latter make decisions where to send a package next according to the criteria (speed, distance, efficiency) of the algorithms inscribed into the routing devices (Dierichs & Pohlmann, 2008), and according to routing tables indicating which networks can be reached via which paths (Tiermann & Goldacker, 2015: 15). It is here where the rules determining how data packages travel through the internet materialise: inscribed into protocols, routers and routing tables.

In the wake of the global surveillance disclosures it was proposed to transform established routing practices: "The idea was to restrict the routing of data between two systems located in country A to systems that are also located in country A. By never crossing into a second judicial territory, your information will be protected by the same privacy laws for its entire journey, bypassing possible snooping attempts from the outside. This concept can be easily expanded from a country to a number of countries" (Pohlmann, Sparenberg, Siromaschenko & Kilden, 2014: 156). The discursive rise of SNR in Germany began when René Obermann - at the time CEO of German telecommunications company *Deutsche Telekom* - took the “Snowden revelations” as an opportunity to present national routing to the public as an easy to implement technical solution of a whole bunch of problems triggered by intelligence practices, among them the “privacy problem” (FAZ.net, 2013). In November 2013, *Deutsche Telekom* gained a strong ally for its proposal: the newly built government coalition explicitly endorsed national routing in its coalition agreement (CDU/CSU/SPD, 2013, p. 147f.). Only a couple of months thereafter the *Federal Minister of Transport and Digital Infrastructure* also recommended to keep data streams within the borders of the Schengen region (Welt.de, 2013). The alliance between the former state-run monopolist *Deutsche Telekom* and parts of the state seems natural enough, as the proposal allows both worlds to translate their interests into one shared overall interest. SNR at this point of the story had become an obligatory passage point (OPP). The latter occurs according to Callon (1986) in a network of relationships between all kinds of heterogeneous elements when an entity manages to position itself in a way so as to redirect the interests of all other entities through its own interest: other entities’ interests are translated in one overall

interest, the OPP. Once established, to pursue their own interests all entities henceforth have to pass through the OPP. This grants entities controlling the latter a great deal of power.

In the case at hand, at the point where *Deutsche Telekom* and the German Federal Ministry of Transport and Digital Infrastructure (BMVI) managed to establish SNR as provisional OPP they were able to claim that all entities that had an interest in the preservation of privacy had to consent to the SNR solution. SNR was a rather convenient OPP for both parties, for it allowed them to reproduce the entrenched routines of the worlds of industry and state: fencing data flows into the territory of the nation state again amounts to reproducing the national container of modern society by infrastructural means and promised to re-install *Deutsche Telekom's* monopolist position. Large infrastructural projects such as this one can be considered traditional undertakings in industrial modernity, which is why representatives of these groups were able to capitalise on established contacts and habits.

We call the governance mode that we come across here *democratic protectionism*. Again, note that we use this term to characterise the style of negotiating privacy in the SNR segment: what is typical for this mode, firstly, is that it features a strong tendency to continue with, and thus *reproduce institutionalised routines*. It locates the threats to privacy and democracy outside the well-established and institutionalised routines of the domestic state and its industrial players. There is no reflexive questioning of domestic institutions, and the public is only called upon to nod the proposal through; the whole constellation does not consider giving the public a voice of its own so as to define the problem, or specify the solution: the well-functioning state and its former monopolist will take care of the problem. The "don't worry, we'll take care of it"-mentality of the proposal mirrors, secondly, protectionism's *lack of transparency:* the issue is settled in ministries and boardrooms.

The *resistance* that the proposal aroused is quite telling. Small and non-German providers' take on SNR was that a law prescribing SNR may harm them and hamper competition; the centralised solution was deemed tantamount to a re-launch of Deutsche Telekom's former monopoly. The conflict furthermore played out in Germany's main IT industrial association BITKOM, which is constituted by German companies as well as global players with subsidiaries in Germany. When BITKOM (2013) desired to compose a position paper in reaction to the surveillance disclosures in 2013, Deutsche Telekom pressed *for* including a passage explicitly *pleading for* SNR. US based companies, however, as the paper was still internally discussed and not yet published, succeeded in attenuating the claim. In the final, published version of the paper, there is only a recommendation to e*xamine* SNR (Wirtschaftswoche, 2014). The conflict mirrors the schism between the modern routines and institutions pertaining to the nation state on the one hand, and globalised infrastructures and economic competition on the other hand.

Yet it seems that democratic protectionism has profound deficiencies in coming to terms with digitally transformed conditions. Quite in contrast to BMVI's energetic endorsement, the *Federal Ministry for Economic Affairs and Energy* (BMWi) and the *Federal Ministry of the Interior* (BMI) raised concerns about the cost-benefit ratio of the proposal, and in some instance even opted against legal regulation. A press release of the BMWi explicitly brought into position the 'open and free Internet' against the 'legal prescription' of SNR (BMWi, 2014, para. 2). The argument went that it was impossible to have "openness" within a SNR system. As matters stood, the algorithmic rules governing routers' decisions to transmit a given IP package so far had not based the decision on whether or not the next possible router was located within national or Schengen territory. While the strategy of the SNR advocates implied to inscribe this rule into the routing system, those who turned against it, although collectively referring to

"openness", did so for very different reasons. Regardless of whether these opponents to SNR had a strategic, instrumental or moral interest in "openness", they could not accept SNR as an OPP and started turning against it. As a result, a rather improbable alliance of opponents emerged, including competition-minded German companies, the global players of the digital economy, the BMWi and BMI – and the *Net-Community* ("*Netzgemeinde*"), i.e. the social world constituted by the core practices of those internet users who establish a reflexive relationship to their own practices. For members of the Net-Community internet usage is not (only) instrumental but meaningful in that it partakes in members' conscious self-constitution. The Net-Community's main concern was that SNR may result in fragmentation of the internet. Thus, whereas there was no agreement on what "openness" actually meant (competition, non-fragmentation) there was nevertheless agreement on the way routers were *not* supposed to make decisions when it came to the transmission of IP packages: on grounds of considering national or Schengen territory. That was already too much of adverse winds for the SNR proposal. The odds were stacked against SNR and as a result the proposal did not occur in the *Digitale Agenda 2014-2017*, the German government's central strategy document on digitisation.

The point that we would like to drive home is that the SNR proposal was so indissolubly tied up with a democratic protectionist style of negotiation that both the proposal and the style of negotiation together did not allow for translation of a sufficient number of (diverse) interests and therefore failed. The proposed solution was rather non-transparent, and stipulated a whole set-up of roles for all those who were involved, including an "external threat" to the well-functioning democratic system herein. For the proposal to have been successful, the location of the enemy "out there" would have needed to be mirrored in the materiality of the routing system: inscribed into the routing tables, algorithms etc. governing the transmission of IP packages. Whereas SNR supporters consequently would have needed a manifold of allies joining the extensive task of re-engineering the current technical structure of the routing system, the negotiation style of protectionism, as it excludes from the outset, does not seem to be appropriate to win those allies over. Having said this, it is not quite easy to maintain the routines of the modern nation-state, nor does it seem to be easily possible to sort "external threats" from "internal shelter." Democratic protectionism has essential difficulties in governing the internet due to the non-reflexive premises it sets out from: *we stay the same while problematic agencies out there have to (be) change(d).* [4]

However, if it is the non-reflexive characteristic of democratic protectionism that is responsible for its disappointment the question arises whether there are arena segments featuring more reflexive modes of negotiation. To deal with this question we will next turn to a segment promising "more reflexivity".

SECTION 3: THE GERMAN PARLIAMENTARY COMMITTEE INVESTIGATING THE "NSA SPYING SCANDAL" (*NSA-UNTERSUCHUNGSAUSSCHUSS*)

Pursuing a comparative research strategy we looked out for a contrasting segment that promised to take up the surveillance disclosures from the angle of the domestic state's internal democratic system. Also, we were looking for a segment which features a governance mode that scrutinises such routines before a wider public.

We opted for analysing the German Parliamentary Committee investigating the NSA spying

scandal (NSA-PIC). Of course, parliamentary investigation committees in general form part of established democratic routines. The NSA-PIC in particular, by setting out from the NSA's activities, additionally seemed to shift the problem to the outside. Yet, a closer look reveals that such a view is mistaken since, theoretically speaking, the role of investigation committees is to actually reflect on (perhaps dysfunctional) institutionalised routines, especially those of government. In this spirit they not only imply the ability of the democratic system to *register* institutional problems but also to *fix* them by initiating processes of self-transformation (e.g. *Wissenschaftlicher Dienst des Bundestags*, 2009, para 2). Thus, such committees are supposed to feature reflexivity and, insofar as the investigation is accomplished in the public gaze, transparency. The setting-up of the NSA-PIC mirrors how the perceived "external threat" triggered the whole investigation, but results in reflexive monitoring. This is already inscribed into the first sentence of the NSA-PIC's mandate where it says that the committee investigates data collection activities of the so-called "Five Eyes" *and* German authorities' (governmental agencies, intelligence services, Federal Office for Information Security) role in this. Thus, there seems great potential in the NSA-PIC to overcome protectionism's non transparent persistence in routines.

Specifying the social worlds involved in the arena we may first note that the nomination request of the NSA-PIC was jointly issued by all parliamentary parties, those that represent government (conservatives and social-democrats) as well as by the outs (leftists and green party). The committee was likewise composed of members of all parties. Hence, the NSA-PIC is constituted by (I.) the social world of governmental parliamentarians (*Regierungsfraktion*) and (II.) the social world of oppositional parliamentarians; at the same time (III.) the social world of government, i.e. the executive body of the state (*Regierungsapparat*) is *object* of the investigation. The same goes for (IV.) the social world of intelligence services, whose members are called upon to act as witnesses, whereas members of (V.) the social world of jurisdiction (constitutional law experts) are heard as experts. The social world of the Net-Community (VI.) meanwhile acts as observer.

To what extent was this arena setting able to overcome protectionism, i.e. to induce reflexive change and provide for transparency? The NSA-PIC at first seemed to keep to its promises in that it addressed time and again the involvement of the German Federal Intelligence Service (BND) and other German authorities in the "Five Eyes'" surveillance activities (Deutscher Bundestag, 2014a, para B. I.). Not only is it NSA-PIC's explicit mandate to investigate authorities' illegitimate participation *in NSA operations*, but also to identify BND's and governmental bodies' *own* transgressions. The NSA-PIC in fact did so. For example, the collaboration between the NSA and BND under the code name *Eikonal* attracted considerable attention and press coverage. Initially unveiled by the media the operation is publicly investigated in the NSA-PIC to this day (SZ.de, 2014). Reports stated that due to the BND's inability to guarantee perfect filtering of internet data streams, data sets were passed on to the NSA which might very well include data regarding German citizens. Additionally, the BND reportedly used highly questionable ways to get permission for this operation from the responsible parliamentary control commission (Deutscher Bundestag, 2014c, p. 75f.). It is transgressions such as these which were disclosed to the public.

Moreover, the whole process effectively induced reflexive change, too. For instance, in November 2015 the government coalition came to an agreement regarding the reform of the BND, including the strengthening of parliamentary control of the intelligence service (Götschenberg, 2015). At this point of the analysis the NSA-PIC seemed to genuinely overcome democratic protectionism: institutional routines were called into question via the system's own

remedy procedures. Instead of aiming to reproduce past structures (territorial society) under contemporary conditions (transnational data flows) by technical means (routing) there was a strong constitution bound mode of identifying problems and solving issues. This is exemplified by a group of legal experts who, when providing a statement before the Committee, were quite explicit about the need to modify the law, including basic rights. One of these experts, former Constitutional court judge Hoffmann-Riem (2014: 55-56) in a paper explicitly stated that territory-bound jurisdiction comes to its limits, given that the routing of data packages was highly contingent on factors other than territory. However, experts did *not* conclude that data flows were to be pushed again into the boundaries of the nation-state; instead *the latter's legal basis was to change*. Again the NSA-PIC arena's potential to induce reflexive change in a transparent way becomes visible, and it is this potential which fundamentally differs from the mode of democratic protectionism.

For us, the occurrence of this potential indicates that there is a different governance mode at work in the NSA-PIC arena. We call this mode *democratic constitutionalism*. The latter strongly appeals to normative democratic principles (e.g. fundamental rights) not only to render the NSA-PIC legitimate (*Deutscher Bundestag*, 2014b, 1821 A), but also to bring *internal* problems to the table without discarding the established system as a whole; instead its core values (whatever they might be in this instance) are reflexively applied.

This finding is not surprising as the governance mode of democratic constitutionalism is by and large very much in line with the way the NSA-PIC is set up formally. What is striking, however, is that it does not manage to *dominate* the segment but is massively hampered by the protectionist mode that also re-emerges here. Protectionist governance practices and discourses in the NSA-PIC include the treatment of the internet as external cause and as issue to be dealt with not by *changing* oneself but by *protecting* oneself (*Deutscher Bundestag*, 2014b, 1816 D); of still more relevance is the fact that subsequent to the official statement of government spokesman Steffen Seibert (2015) that the BND had in fact "technical and organisational deficiencies", a discourse emerged that claimed the strengthening of BND's independence from the NSA. As a consequence, some even demanded to equip BND with more financial resources to *expand* the institution. And while we cannot provide evidence that this was indeed triggered by the "independence-from-the-NSA" discourse BND's and other intelligence service's staff was increased by 500 between June 2013 (Snowden revelations) and November 2015 (Netzpolitik.org, 2015).

Our interpretation of these events is that the negotiation of privacy in the NSA-PIC somewhat *oscillates* between the modes of democratic protectionism and constitutionalism. Connecting this diagnosis back to the social worlds analysis we can see that as a result of this oscillation there are committee members who are torn into two directions at the same time: those who belong to the governing coalition are simultaneously a) part of the forces that strive to render events transparent and induce reflexive change, and as they also form part of the very social world that is bound to come under scrutiny (government), b) of antipodal forces. While the social world of the Net-Community does not act as a political pressure group, but mainly observes and registers, the social world of jurisdiction might *appeal* to political decision makers – but this is insufficient to tip the balance in favour of the constitutionalist forces. [5] In this sense, what the analysis reveals is the *limits of constitutionalism*: procedures in the investigation committee in one way or another are still bound to the routines of the established institutions pertaining to the territorial state. Constitutionalist governance time and again gets stuck; for, while it is possible for this mode to radically call into question institutionalised governmental routines it is not able to also substantially modify these routines; part of the

problem is that if constitutionalism did so, it would potentially threaten its own conditions of existence.

Thus, while there is some potential for reflexive, transparent change to be detected in the NSA-PIC segment of the privacy arena, the segment still seems to be bound too strongly to the routines of the nation state. This raises the question for future research: are there arena segments that feature comparable reflexivity and transparency while being less closely tied to the nation-state?

CONCLUSION

We would like to make a case for the methodology applied here by briefly summarising the main points made above. First of all, the methodology presented above seems appropriate for studying the public renegotiation of privacy as a way of doing internet governance, for it allowed us to identify key parameters of the democratic styles coining these negotiations: transparency vs. opaqueness and the persistence in routines vs. embracing reflexive change. While social worlds/arenas theory enables one to focus on technical, legal, political etc. governance "solutions" on a level playing field the comparative strategy also permits to contrast cases according to a certain set of parameters named above.

Future research might continue the search for arenas that promise transparency and reflexivity without being as much hampered by the persistence in the routines of the nation-state. However, drawing on the parameters in a more analytical vein also helps to systematically speculate on further governance modes to be encountered within the overall privacy arena. Now, if democratic protectionism (non-transparency plus persistence in routines) and constitutionalism (transparency plus persistence in routines) continue to generate obstruction, logically there remain two future paths: if actors not bound to democratic routines (e.g. economic ones) step in by non-transparently negotiating backroom decisions with enfeebled politics, negotiations may acquire a *post-democratic* character (non-transparency plus non-boundedness to democratic routines). The more optimistic option would be the rise of an *experimental* governance mode (transparency plus non-boundedness) that neither starts in providing fixed problem definitions nor provides ready-made solutions. Which modes are going to prevail or mix in the future only time will tell; however, the methodology presented here will enable us to understand the trajectories of the privacy arena.

REFERENCES:

Bitkom (2013, October 31). *Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit*. Retrieved from https://www.bitkom.org/Publikationen/2013/Positionen/Positionspapier-zu-Abhoermassnahmen/BITKOM-Positionspapier-Abhoermassnahmen.pdf

BMWi (2014, June 13). Staatssekretär Kapferer: Offenes und freies Internet erhalten, Pressemitteilung vom 13.06.2014. Retrieved from http://www.bmwi.de/DE/Presse/pressemitteilungen,did=642114.html

Büttner, B., Geminn, C., Hagendorff, T., Lamla, J., Ledder, S. Ochs, C., & Pittroff, F. (2016). *Die Reterritorialisierung des Digitalen: Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden*. Kassel: Kassel University Press. Retrieved from http://www.uni-kassel.de/upress/online/OpenAccess/978-3-86219-106-2.OpenAccess.pdf

BMWi/BMI/BMVI (2014, August 20). *Digitale Agenda 2014-2017 (English version)*. Retrieved from http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf

Callon, M. (1980). Struggles and negotiations to define what is problematic and what is not. The socio-logic of translation. In K.D. Knorr-Cetina, R. Krohn & R. D. Whitley (Eds.), *The Social Process of Scientific Investigation: Sociology of the Sciences Yearbook* (pp. 197-220). Dordrecht, Holland: Reidel.

Callon, M. (1986). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fisherman of St. Brieuc Bay. In J. Law (Ed.), *Power, Action, and Belief. A New Sociology of Knowledge?* (pp. 1996-233). London, England: Routledge & Kegan Paul.

Callon, M., Lascoumes, P. & Barthe, Y. (2011). Acting in an Uncertain World. An Essay on Technical Democracy. Cambridge, MA/London: MIT Press.

CDU/CSU/SPD (2013). *Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18 Legislaturperiode*. Retrieved from https://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf

Clarke, A. (1991). Social Worlds Theory as Organizational Theory. In D. Maines (Ed.), *Social Organization and Social Process: Essays in Honour of Anselm Strauss* (pp. 17-42). Hawthorne, NY: Aldine de Gruyter.

Clarke, A. & Leigh Star, S. (2008). The Social Worlds Framework: A Theory/Methods Package. In: E.J. Hackett, O. Amsterdamska, M. Lynch & J. Wajcman (Ed.), *The Handbook of Science and Technology Studies*. 3rd Edition (pp. 113-137). Cambridge, MA/London: MIT Press.

Deutscher Bundestag (2014a). Drucksache 18/ 843 18. Wahlperiode. Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE und BÜNDNIS 90/DIE GRÜNEN. Einsetzung eines Untersuchungsausschusses. Retrieved from http://dip.bundestag.de/btd/18/008/1800843.pdf

Deutscher Bundestag (2014b). Plenarprotokoll 18/23. Stenografischer Bericht. 23. Sitzung. Rede: Untersuchungsausschuss zur Überwachungsaffäre, Plenarsitzung. Retrieved from

http://dipbt.bundestag.de/dip21/btp/18/18023.pdf

Deutscher Bundestag (2014c). Transcript: Bundestag Committee of Inquiry into the National Security Agency [Untersuchungsausschuss ("NSA")], Session 24 WikiLeaks release: 12, May 2015. Retrieved from https://wikileaks.org/bnd-nsa/sitzungen/2401/WikiLeaksTranscriptSession2401fromGermanNSA_Inquiry.pdf

Dewey, J. (1946). The Public and its Problems. An Essay in Political Inquiry. Denver: Swallow.

Dierichs, S. & Pohlmann, N. (2008). So funktioniert Internet-Routing. Retrieved from http://www.heise.de/netze/artikel/So-funktioniert-Internet-Routing-221495.html?view=print

Dönni, D., Machado, G.S., Tsiaras, C. & Stiller, B. (2015). Schengen Routing: A Compliance analysis. In Latré, S.,Charalambides, M. Francois, J., Schmitt, C. & Stiller, B. (Ed.), *Intelligent Mechanisms for Network Configuration and Security, Proceedings* (pp. 100-112). Heidelberg et al.: Springer.

Faz.net (2013, November 2013). Im Gespräch: René Obermann und Frank Rieger. Snowdens Enthüllungen sind ein Erdbeben. *Frankfurter Allgemeine Zeitung*. Retrieved from http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/im-gespraech-rene-obermann-und-frank-rieger-snowdens-enthuellungen-sind-ein-erdbeben-12685829.html

Glaser, G. B., & Strauss, A. L. (1998). *Grounded Theory. Strategien qualitativer Forschung*. Bern, Switzerland: Hans Huber.

Götschenberg, M. (2015). Einigung auf Geheimdienstreform. Koalition nimmt BND an die Leine. *Tagesschau*. Retrieved from https://www.tagesschau.de/inland/bnd-reform-101.html

Hoffmann-Riem, W. (2014). Freiheitsschutz in den globalen Kommunikationsinfrastrukturen. In: *Juristen-Zeitung*, 69, 53-63.

Lamla, J. (2013). Arenen des Demokratischen Experimentalismus. Zur Konvergenz von nordamerikanischem und französischem Pragmatismus. *Berliner Journal für Soziologie*, 23(3-4), 345-365.

Netzpolitk.org (2015). 500 neue Stellen für BND, Verfassungsschutz & Co. Retrieved from https://netzpolitik.org/2015/500-neue-stellen-fuer-bnd-verfasungsschutz-co/

Ochs, C., & Ilyes, P. (2014). Sociotechnical Privacy: Mapping the Research Landscape. Tecnoscienza. *Italian Journal of Science & Technology Studies, 4*(2), 73-91.

Pinch, T., & Leuenberger, C. (2006). Studying Scientific Controversy from the STS Perspective. Paper presented at the EASTS Conference "Science Controversy and Democracy. Retrieved from https://www.researchgate.net/publication/265245795StudyingScientificControversyfromtheSTS_Perspective

Pohlmann, N., Sparenberg, M., Siromaschenko, I. & Kilden, K. (2014). Secure Communication and Digital Sovereignty in Europe. Highlights of the Information Security Solutions Europe 2014 Conference. In Reimer, H., Pohlmann, N., Schneider, W. (Ed.), *ISSE 2014 Securing Electronic Business Processes* (pp. 155-169). Heidelberg et al.: Springer.

Schaar, P. (2009). *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*. München: Goldmann.

Seibert, S. (2015). *Fernmeldeaufklärung des Bundesnachrichtendienstes, Press release*. Retrieved from https://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2015/04/2015-04-23-bnd.html

Strauss, A. L. (1978). A Social World Perspective. *Studies in Symbolic Interaction*, 1, 119–128.

Strauss, A. L. (1982). Social Worlds and Legitimation Processes. *Studies in Symbolic Interaction*, 4, 171-190.

Strauss, A.L. (1993). *Continual Permutations of Action*. Hawthorne, NY: de Gruyter.

Süddeutsche Zeitung (2014, October 4). Codewort Eikonal - der Albtraum der Bundesregierung. Retrieved from http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432

Tiermann, J. & Goldacker, G. (2015). Vernetzung als Infrastruktur – Ein Internet Modell. Fraunhofer FOKUS: Berlin.

Welt.de (2013). Deutschland muss eine Aufholjagd starten, Interview mit Alexander Dobrindt. Retrieved from http://www.welt.de/politik/deutschland/article123773626/Deutschland-muss-eine-Aufholjagd-starten.html

WirtschaftsWoche (2014). Echte Zerreißprobe. *WirtschaftsWoche*, 8/2014, 52-54.

Wissenschaftlicher Dienst des Bundestags (2009). Aktueller Begriff. Untersuchungsausschüsse. Retrieved from https://www.bundestag.de/blob/190568/ce3840e6f7dbfe7052aa62debf812326/untersuchungsausschuesse-data.pdf

FOOTNOTES

1. The framework can only be sketched here in general terms. For a detailed blueprint see Lamla (2013). Readers familiar with the STS literature may note that this approach falls into line with pragmatist minded STS investigations of the relation between technoscience, the public and democratic politics as accomplished by Callon, Latour, Marres and others.

2. What we present here is work in progress; while we limit our presentation to two cases we have also analysed a third one, the European General Data Protection Regulation.

3. In 2008 Dierichs and Pohlmann estimated that the internet consisted of about 110,000 AS (Dierichs & Pohlmann, 2008).

4. Interestingly, the basic strategy that aims to maintain the sovereignty of the nation state under digitised circumstances has not entirely disappeared, but was somehow shifted. SNR may be understood as an attempt to reterritorialise information flows that threaten to exceed certain territories, and while the routing strategy was discredited, in the Digitale Agenda digital sovereignty is still one of the goals the government strives to achieve (BMWi, BMI, and BMVI, 2014: 4). In this sense, we might say that the strategy of reterritorialisation managed to survive in a new guise, once it was not tied to routing anymore (for more information, see Büttner et al., 2016: 149-151).)

5. Note that, as "constitutionalism" refers to a governance mode, it may not be identified with one particular social world. Accordingly, it is not only the judges who foster constitutionalist forces, but also, say, the green party (opposition) member of parliament Konstantin von Notz who frequently argues in a constitutionalist style.