Article

The Norwegian Data Inspectorate: Between Governance and Resistance

Kjersti Lohne

Peace Research Institute Oslo / Department of Criminology and Sociology of Law, University of Oslo, Norway.
kjersti.lohne@jus.uio.no

Abstract

The growing impact of information and communication technologies has resulted in the establishment of data protection authorities across Europe. Despite the role of these bodies as enforcers of privacy and data protection legislation, Surveillance Studies has so far offered little attention to their role in resistance. Based on a critical socio-legal examination of the Norwegian Data Inspectorate, the focus of this article is on the role of data protection authorities in resisting surveillance and threats to privacy and data protection. More specifically, the article asks what power the Norwegian Data Inspectorate has to achieve genuine resistance, and how its institutional structure affects this capability. Through a three-pronged analysis consisting of (i) institutional mapping, (ii) a typology of resistance strategies, and (iii) a review of its role in the Norwegian public debate on the EU Data Retention Directive, the article addresses the fundamental tension inherent in the Norwegian Data Inspectorate as a privacy-advocating ombudsman and an administrative body. As such, the research shows how, and to what extent, its institutional structure both strengthens and limits its possibilities for resistance.

The growing impact of information and communication technologies has resulted in the establishment of data protection authorities across Europe. According to Article 28 in the EU Directive 95/46/EC, each member state within the European Economic Area (EEA) shall provide one or more public supervisory authorities endowed with investigative powers, effective powers of intervention, and the power to engage in legal proceedings to ensure adherence to data protection regulations. In response to similar developments, Surveillance Studies has developed into a disciplinary field in its own right, tending, stretching and dismantling the ‘panoptic straightjacket’ and ‘Big Brother’ metaphors in efforts to conceptualize how surveillance technologies permeate an ever-increasing range of social life (see Coleman 2011; Lyon 2006; Marks 2002). Based on a critical socio-legal examination of the Norwegian Data Inspectorate (NDI), the focus of this article is on the role of data protection authorities in resisting surveillance and threats to privacy and data protection. More specifically, the article asks what power the NDI has to achieve genuine resistance, and how its institutional structure affects this capability. Through a three-pronged analysis consisting of (i) institutional mapping, (ii) a typology of resistance strategies, and (iii) a review of its role in the Norwegian public debate on the EU Data Retention Directive, the article addresses the fundamental tension inherent in the NDI as a privacy-advocating ombudsman and an administrative body. As such, the research shows how, and to what extent, the NDI’s institutional structure both strengthens and limits its possibilities for resistance.

Taking a predominantly normative stance, scholars in Surveillance Studies direct their attention towards the legitimate need to resist surveillance, while less academic scrutiny focuses on describing *how*

contemporary resistance is enacted.¹ Important exceptions include Bennett (2008), Martin et al. (2009), Marx (2009), and Introna and Gibbons (2009). While their work makes a substantial contribution to a conceptualization of resistance within Surveillance Studies, in particular by drawing attention to the significance of privacy advocates, the way administrative bodies such as data protection authorities resist surveillance has remained strangely exempt from analysis, with the exception of David H. Flaherty's seminal study from 1989.² It may be, as suggested by Introna and Gibbons (2009, 238), that such bodies are 'often seen as too close to government to be an effective mechanism of resistance', or, that their presence causes 'a false sense of security' and in consequence legitimates the development of surveillance societies (Flaherty 1989, 11). Another explanation may be found in a particular methodological bias: in the case of scholars inclined to think 'critically' about state power, especially with regard to surveillance issues, a generally positive attitude towards the work of data protection authorities may lead to a preference for objects of study more readily—and justifiably—subject to criticism. However, while these suggestions help explain the lack of attention towards the role of data protection authorities, they also express the inherent *duality* of these bodies: although independent, data protection authorities are state actors yet at the same time, critics of state practices (Flaherty 1989).

Since its establishment in 1980, the NDI has played a significant role in the Norwegian discourses on privacy, data protection and surveillance. Alongside its supervisory responsibilities as a state administrative body, the NDI's mandate is to act as an ombudsman for the interests of privacy and data protection.³ Although there has been some dissatisfaction with such a broad mandate, this particular institutional arrangement also provides the NDI with considerable access to the public discourse. Besides numerous consultative statements requested by state authorities on issues of privacy and data protection, its expertise and opinion is called for and disseminated through various public appearances by its representatives in the media, seminars and debates. Throughout the past decades, there has been a steady increase of administrative supervision in Norway as elsewhere. Whether the growth represents an increase in de facto supervisory activities, or results from general developments in government administration such as the expansion of administrative law in tandem with the prevailing juridification of society, remains questionable (Stub 2010).⁴ Through a mapping of the NDI's development from 2000 – 2010, this article sheds light on some additional aspects of this discussion by inquiring into the nature of the NDI's growth. How data protection authorities interpret and perform their tasks and responsibilities necessitates critical reflection. Does the NDI's institutional development mirror its role as a privacy-advocating ombudsman, or that of an administrative supervisory body?

The research strategy has involved a review of core regulatory and official reports, consultative statements and annual reports from the NDI in the years 2000 – 2010. As official sources, these documents possess methodological credibility and validity; but they are also normative and performative remnants, requiring a critical distance in their analysis (Kjeldstadli 1999). To this end, the research has included an analysis of

¹ The normative perspective is maintained in the 2009 special issue of *Surveillance & Society* on 'the interplay between surveillance and resistance, asking if surveillance can be successfully resisted, and, if so, how this resistance might look' (Fernandez and Huey 2009, 198).

² *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Flaherty 1989) offers a thorough and comparative review of data protection and surveillance, including the implementation of data protection laws and organizations of data protection agencies.

³ The English translation of the NDI's name also reflects the duality of its mandate: While *The Data Protection Agency* connotes its role as a watchdog, *The Data Inspectorate* accentuates its control function. This author's use of the latter is not intended to accentuate either of these roles, but rather to comply with the agency's own use of the English translation on their web sites.

⁴ Nonetheless, research is beginning to grapple with the implications of the accumulation of power by administrative agencies: As Stub's (2010) work on regulatory enforcement in Norwegian administrative law demonstrates, supervisory bodies may resemble quasi-judicial agencies, but with fewer procedural safeguards than there are in criminal law procedures. See inter alia Christensen et al. (2002); Power (1997).

a semi-structured interview with the NDI's former director Georg Apenes, as well as of seminars, debates and media reports on privacy issues, particularly concerning the EU Data Retention Directive.

The article proceeds in three parts. The first section presents the NDI as an institution and a state administrative body, addressing the parameters of its mandate, size and responsibilities. Providing the empirical background for the succeeding analysis, the mapping is also a reflection of how the trajectory of security thinking and ICT has altered the landscape of privacy and data protection since the beginning of the 21st century. Part two probes into the NDI's practices of governance and resistance. It builds on a fourfold typology developed by Keck and Sikkink (1998) to describe the tactics employed by transnational advocacy networks: information politics, leverage politics, accountability politics and symbolic politics, which Bennett (2008) has adapted and applied to the study of privacy advocates. This juxtaposition will shed light on whether, and to what extent, the NDI's practices resemble those of privacy advocates, and hence, how the NDI manages its twofold role in resisting surveillance and threats to privacy and data protection. The latter is also the subject of the third and final part, where a delineation of the NDI's role in the high-profile debate on the EU Data Retention Directive illustrates the inherent tension stemming from the NDI's institutional twofold role.

The Norwegian Data Inspectorate

The Norwegian Data Inspectorate (NDI) was set up 1 January 1980 to prevent violations of the right to privacy and the misuse of personal data, following the 1978 Personal Data Register Act. Through the adoption of EU Directive 95/46/EC, the act was replaced in 2001 when the current Personal Data Act (PDA) came into force. The purpose of the PDA is to 'ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality' (Personal Data Act 2000, Section 1(2)). In addition, it regulates the NDI's organization and mandate,⁵ establishing its independence as an 'independent administrative body subordinate to the (sic.) King and the Ministry' (Personal Data Act 2000, Section 42(1)).⁶ Generally, its decision can be appealed to the Privacy Appeals Board, also regulated by the PDA to ensure due process guarantees.

The NDI has five departments: administration, information and external relations, security and supervision, legal guidance, and a legal department. Besides the PDA, it also regulates compliance with the Health Registers Act of 2001.⁷ To illustrate the NDI's structural development since the inception of the PDA and throughout the past decade, the table below gives an overview of its budget and permanent employment contracts from 2000 – 2010.

⁵ 'The Data Inspectorate shall 1) keep a systematic, public record of all processing that is reported...or for which a license has been granted..., 2) deal with applications for licenses, receive notifications and assess whether orders shall be made in cases where this is authorized by law, 3) verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified, 4) keep itself informed of and provide information on general national and international developments in the processing of personal data and on the problems related to such processing, 5) identify risks to protection of privacy, and provide advice on ways of avoiding or limiting such risks, 6) provide advice and guidance in matters relating to protection of privacy and the protection of personal data to persons who are planning to process personal data or develop systems for such processing, including assistance in drawing up codes of conduct for various sectors, 7) on request or on its own initiative give its opinion on matters relating to the processing of personal data, and 8) submit an annual report on its activities to the King' (Personal Data Act 2000, Section 42(3)).

⁶ At the present time (2012), the NDI sorts under the Ministry of Government Administration and Reform.

⁷ Formally known as the Personal Health Data Filing System Act (2001).

Year	Budget (NOK)	Permanent Contracts
2000	15 633 000	23
2001	18 413 000	26
2002	17 800 000	27
2003	18 300 000	26
2004	21 000 000	27
2005	23 000 000	31
2006	24 778 000	32
2007	25 000 000	33
2008	26 000 000	35
2009	29 020 000 + 4 948 000	36
2010	31 000 000 + 4 000 000 ⁸	37

Table 1: The NDI's budgets and permanent contracts, 2000 – 2010.⁹

The table shows that the NDI's budget has just about doubled over the past ten years. The number of employees, measured by permanent work contracts, has seen a considerable increase (61 per cent). Even taking account of the healthy state of the Norwegian economy, and omitting temporary engagements from analysis, the numbers above make clear that the NDI has undergone significant institutional growth. Hence, in what follows, the article offers some tentative explanations of the Norwegian administrative and bureaucratic extension of privacy and data protection, and probes into how resources are balanced between the administrative and ombudsman functions of the NDI. To this end, this inquiry engages in a discussion of contemporary conceptions of the threat landscape of privacy and data protection, in which the NDI occupies centre stage.

An inquiry into the Norwegian Data Inspectorate's development

A reading of the NDI's annual reports shows the shift in the regulatory framework following the adoption of the PDA in 2001.¹⁰ Although the PDA will generally resemble the one it replaces, the NDI (2001) reports that the new legislation will introduce new responsibilities: in addition to informing the public of *how* the legislation works, an explanation of *why* privacy and data protection is important in the first place is also necessary. These responsibilities are part of the NDI's function as ombudsman; hence, there is reason to look into the extent to which the PDA has enhanced this role as against its administrative and supervisory responsibilities.

The table below presents an overview of the NDI's casework from 2000 – 2010, delineated in: (i) licenses granted for use of personal data; (ii) notifications received of use of personal data; (iii) consultative statements and annotated consultative statements (where this information is provided); and (iv) appeals and number of cases overturned in whole or in part.

The statistically deviant number of licenses granted in 2000 is an indication of the different administrative practices in the 1978 Personal Data Registers Act and the 2001 Personal Data Act. Accentuating a shift from a priori supervision to inspections and follow-ups, the PDA relies largely on *notifications* rather than *license work*, in contrast to its predecessor. In cases involving particularly sensitive information however, licenses are still required. The number of licenses granted peaks, except for 2001, towards mid-decade,

⁸ The additional resources for 2009 and 2010 are reserved for specific projects (NDI 2011b).

⁹ The budget figures are not corrected for inflation and wage levels.

¹⁰ The data illustrates the development of practice following the immediate coming into force of the PDA, its adaption process and how it is a decade on; it cannot, however, stand as a valid comparison to the legislation it replaces, other than by providing a comment and reflection upon the sources' own evaluations.

before declining. The NDI (2005) explains the high number in 2004 by referring to its use of standardized licenses, for instance for banks, research projects etc., an explanation also given regarding administrative practices prior to the coming into force of the PDA (NDI 2001). The following year, the NDI (2006) reports that, as the majority of licenses concern research projects, legal amendments will be made to exempt certain projects from this requirement, intended to reduce the workload. Consequently, the Health Research Act came into force in 2009, which the NDI (2010) recognizes to have had the intended effect of reducing the caseload. Nonetheless, in 2010, the number of licenses granted is once more almost as high as mid-decade.¹¹

Year	Licenses granted	Notifications received	Inspections	Consultative statements/ Annotated	PAB; appeals & overturned ¹²	
2000	2,150	-----	19	unspecified/105	-----	
2001	166	2,494	53	unspecified/89	1	0
2002	437	9,748	104	unspecified/67	6	1
2003	470	6,210	79	135/unspecified	6	2
2004	817	2,777	161	124/104	6	3
2005	403	2,953	130	139/88	9	5
2006	225	3,019	150	123/85	15	7
2007	237	2,952	134	Unspecified	7	1
2008	206	2,910	141	Unspecified	6	3
2009	195	3,778	168	162/87	25	8
2010	357	3,693	135	123/approx. 70	11	6

Table 2: The NDI's executive casework and appeals, 2000 – 2010.

The table's second column also reflects the administrative shift following a change in privacy and data protection legislation. The high number of notifications of use of personal data in 2002 marks the closing date for notifying the NDI of existing licenses in need of verification. In December 2002, the NDI (2003) received more than 300 notifications concerning use of personal data. Thus, after an initial peak following the coming into force of the PDA, the number of notifications roughly stabilizes between 2,700 and 3,700 notifications annually. Commenting on an admittedly minor yet *de facto* decline, the NDI (2009) writes that this is probably the result of locally established Data Protection Officials at various companies and enterprises, their presence leading to exemption from the obligation to notify the NDI of its use of personal data.

While the NDI (2002) reports that an intended consequence of the administrative shift is to focus resources on inspections, information and counseling, a closer look at the NDI's inspection activities suggests that, although this work has seen an increase, this development cannot alone account for the resources liberated by the legal amendments. Inspection visits build up unevenly in the first half of the decade, a development in line with the other administrative activities discussed so far. In the latter part of the decade, inspections somewhat stabilize between 134 and 168 inspections annually. However, what is not apparent from these numbers is yet another administrative adjustment: in 2004, the NDI introduces inspections *by letter* as a supplement to inspections on-site (2005). In the annual reports thereafter, it is not possible to tell how many of the inspections reported are by letter and how many are not.

Bearing in mind the institutional growth illustrated in Table 1, it appears that the underlying facts of the NDI's budgetary boost and rise in employment rates are not reflected in its administrative processing of

¹¹ The NDI does not report the total number of applications for licenses—only those granted.

¹² Data is collected from Difi (2011) and the Public Commission on Privacy and Data Protection (NOU 2009:1) and is randomly crosschecked with a sample of annual reports from the Privacy Appeals Board.

licenses and notifications. Nor does the increase in inspections appear significant enough to legitimate the NDI's growth. In fact, one could argue that administrative casework is reduced through law making, and by disclaiming liability through regulative delegation or standardization. Hence, the NDI's ombudsman function may be interpreted as accounting for the majority of the NDI's growth, arguably even eating into its administrative roles.

Such a development is supported by the NDI (2010) who report that their work with consultative statements is particularly time consuming, especially as they often involve novel challenges and issues that may demand considerable attention, such as the introduction of new technologies or new legislation. However, the NDI's activities in pursuing the interests of privacy and data protection are significantly more difficult to operationalize quantitatively than its administrative casework: The data in Table 2 neither give an adequate measure of whether the work on consultative statements has increased or not, nor on the amount of time spent on each consultative statement.

The final column shows the annual number of appealed cases dealt with in the Privacy Appeals Board (PAB), and the number of cases overturned in whole or in part. The number of cases dealt with each year varies greatly, ranging from one case in the PAB's first year of work to 25 cases in 2009, yet with the medium and mode value of six cases per year. According to the NDI (2009, 14), the cases that are overturned by the PAB represent areas where the legislation is unclear and in need of additional judicial interpretation and procedure. In the Public Commission on Privacy and Data Protection's discussion of the issue, they 'do not wish to speculate about the causes for any legal differences' but rather draw attention to the significant percentage of decisions that are altered, although 'relatively few cases are appealed' (NOU 2009:1, 205).¹³ According to the commission, the high level of changed decisions represents unpredictability in case processing and therefore a potential obstacle to due process guarantees. However, the paper argues below that this discussion is rather symptomatic of a certain tension in the institutional arrangement of the data protection authorities and in particular in the twofold role of the NDI as both a supervisory body and an ombudsman.

The Norwegian Data Inspectorate as Ombudsman

The NDI recognizes its responsibilities as an ombudsman for privacy and data protection as particularly important (inter alia NDI 2010). Traditionally, an ombudsman ensures individual rights vis-à-vis public and state power, albeit their decisions are limited to an advisory or informative character. In Norway, an ombudsman is generally employed in the public administration to strengthen and defend minority groups or interests, such as the Children's Ombudsman and the Equality and Anti-discrimination Ombudsman (NOU 2009:1). However, as recalled by Melton (1991, 202), '[r]esponding to complaints from the public, the ombudsman "has the power to investigate, criticize and publicize, but not to reverse, administrative action"'. For instance, the power of the Ombudsman in relation to the Norwegian Parliament is not found in any privileged measures of administrative enforcement, but is rather contingent upon its inherent authority, which at most times ensures that the public administration is attentive to whatever criticism the Ombudsman may voice (Boe 1993).

However, with the NDI being an administrative supervisory body as much as an ombudsman, these definitions do not sufficiently describe the powers and practices of the NDI. While an ombudsman serves to protect particular interests, administrative supervision entails a duty and responsibility to be attentive, inspect and intervene in the case of incorrect and irregular conduct. As is clear from the Public Commission on Privacy and Data Protection's report (NOU 2009:1), the commission finds the dual nature of the NDI to be an ambiguous and a somewhat problematic feature, and links this to the above discussion on the high rate of decisions reversed by the Privacy Appeals Board. The report states: 'in some circumstances it can be unfortunate that the balance of interest is determined by an organization that

¹³ Unless specified, all translations are by the author.

perceives its responsibilities to guard one particular interest above others' (NOU 2009:1, 205). The majority in the commission conclude that the institutional duality of the NDI in terms of administrative supervision and the ombudsman function should be maintained, yet a minority dissent nevertheless illustrates the tensions and disagreements that are lurking beneath the surface regarding the NDI's structure, *and* within an officially appointed committee. The report's suggestion that a separate council should be established 'to ensure that other interests as well as privacy and data protection are sufficiently emphasized' therefore emerges as an attempt to suppress this tension rather than as a coherent proposal from a joint committee (NOU 2009:1, 208).¹⁴

The far-reaching importance of the fact that the NDI's mandate consists of two incompatible roles emerges clearly from this delineation of its institutional nature. Yet is there always an inherent discrepancy between the supervisory and ombudsman function of the NDI? On the one hand, there are grounds for claiming that they may weaken each other; this particular merging of responsibilities raises important questions concerning a conflict of interest and authority. The NDI identifies threats to privacy and data protection, and gives advice on how to prevent or limit these threats. Such a role enables it to offer normative guidance beyond what typically characterizes an administrative body in Norway. The same body that exercises authority by enforcing the PDA simultaneously makes individual decisions on the use of personal data, such as granting licenses. This presupposes a balance of interests that because of the NDI's role as ombudsman—a promoter of privacy and data protection—it may lack. To champion the cause of privacy and data protection while at the same time ensuring just processing may conflict with standards of objective validity that elsewhere characterize legal protection and due process guarantees. On the other hand, there might also be significant strengths in the particular mandate of the NDI. For example, through administrative inspections and casework, the NDI gains access to information that is invaluable in its role as an ombudsman.¹⁵ The NDI's first-hand knowledge of how privacy and data protection issues come into play in real life may in fact only increase their competence and credibility as a promoter and public watchdog of privacy and data protection.¹⁶ The next section therefore focuses on the interplay between these two roles in the NDI's practices of resistance: how they may both weaken and strengthen the NDI's capacity for genuine resistance, and if so, under what circumstances.

A Typology of Tactics: Resisting Governance or Governing Resistance?

In spite of the tensions apparent from examination of the NDI's role as an administrative supervisory body, the explorations of its mandate and practices have nonetheless underlined the fact that its institutional and bureaucratic character is that of state apparatus. The NDI holds legal authority and consequently has power to administer and impose sanctions. It is a regulatory body, an administrator and an agent of governance—the NDI *practices* state governance. This section will probe deeper into how this governance operates by examining to what extent the NDI employs strategies of persuasion and pressure generally reserved for advocacy networks without traditional forms of power, i.e. institutionalized power such as that of the NDI. It builds on a fourfold typology developed by Keck and Sikkink (1998) to describe the tactics employed by transnational advocacy networks: information politics, leverage politics, accountability politics and symbolic politics, which Bennett (2008) has adapted and applied to the study of privacy advocates.¹⁷ This juxtaposition will shed light on whether, and to what extent, the NDI's practices

¹⁴ Schartum (2008) has suggested relieving this tension by creating sector-specific authorities which would provide a more integrated practice.

¹⁵ Occasionally, inspections may also be an enactment of the NDI's ombudsman role, for instance in response to citizen complaints.

¹⁶ This is also a view adopted by the NDI themselves in a recent strategy document (NDI 2011a, 17). Here, the NDI also responds to questions regarding their double role (cf. NOU 2009:1; Difi 2011).

¹⁷ Limitations apply as this typology originally characterizes *networks* and not individual organizations such as the NDI.

resemble those of privacy advocates, and hence, how the NDI manages its twofold role in resisting surveillance and threats to privacy and data protection.

Information politics

Central to the effectiveness of any transnational advocacy network, is the ability to generate accurate information and use it where it will have the most impact (Keck and Sikkink 1998). Yet in contrast to the ‘human rights methodology’, where facts and testimonies of human rights abuses are applied to induce those in power to ‘do something’, the politics of information are handled in a slightly different manner by privacy advocates. Instead of reporting actual harms, ‘[i]t relies upon argumentation about potential consequences’ (Bennett 2008, 98).

Throughout its annual reports, the NDI increasingly draws attention to personal data as raw material, or currency, applied and used in direct marketing, crime and terrorism. At the start of the decade, the NDI (2002) announces that the core issue of privacy and data protection in the 21st century will concern information. Almost a decade later, the NDI (2011b, 27) has grown especially attuned to the growing ‘app’ market for smart phones, emphasizing that companies engaged in the industry ‘are not charity organizations, but companies that make money out of personal information generated by their users’. They warn of the dangers of a situation in which inadequate information security and liberal data collection practices create a “‘running buffet” for identity thieves’ (2008, 26), pointing out that the greater the amount of information collected about a particular individual, the greater the chance will be of this individual having his or her identity stolen. Thus, the NDI emphasizes the importance of building critical awareness to prevent victimization, and does this by providing information and reports on both actual and potential consequences of unwise practices.

In response to the recent criminalization of preparatory acts such as child grooming,¹⁸ and ‘intention to make associations to conduct terrorism’,¹⁹ the NDI reports that, although it acknowledges the need for new law enforcement tools to keep track of technological developments, it has concerns regarding contemporary state practices of ‘precautionary justice’, i.e. meting out punishment in anticipation of wrongdoing. Making reference to fundamental democratic legal principles (thus engaging in moral leverage as well, discussed next), the NDI (2007, 31) warns that ‘to search for a perpetrator that has not broken the law, but intends to break it, may quickly result in a type of surveillance that also affects a great number of innocent people’. Another implication identified by the NDI regarding the ‘pre-emptive trend’ in law enforcement is a faith in the law’s ability to prevent crime and other social harms. In a consultative document on the criminalization of child grooming, the NDI claims that the dominant issue concerning children and ICT is the lack of adequate knowledge, or ignorance, of parents or guardians. Thus the NDI (2006) argues that attention and resources should be directed towards consciousness building instead of legal regulations, which, they claim, may also have the unintended effect of encouraging parents to assume that their children are adequately protected, and so further reducing parents’ engagement with their children’s ICT use.

Raising awareness of the potential costs and consequences of the misuse of personal data is central to the NDI as part of ‘educating’ the public. Multiple programs have been established, for example: (i) a teaching scheme for children and young people aiming to increase their responsibility and respect for themselves and others on-line; (ii) a local ombudsman system (Data Protection Officers) in local companies and enterprises; and (iii) a ‘low threshold’ service that provides assistance in the case of on-line violations (2011b).²⁰ In addition, the NDI participates actively in a variety of debates and forums, as

¹⁸ Child grooming refers to actions conducted with the purpose of lowering a child’s resistance to sexual exploitation. In 2007, child grooming was criminalized through a legal amendment to the Norwegian Penal Law, § 201a.

¹⁹ Norwegian Penal Code, Art. 147 a.; introduced into the Code in 2002.

²⁰ Translated from Norwegian: *Undervisningsopplegget Du Bestemmer, Personvernombud, Slettmeget.no*.

well as using its websites to provide information to the public. This dissemination work, or information politics, has brought the NDI numerous awards, one of which being given by an association of public relations and communications consultancies (2009).²¹

Information politics chooses the route of persuasion; it is about ‘speaking truth to power’ (Bennett 2008, 96). Nonetheless, as an ombudsman for privacy and data protection, ‘information politics’ constitutes an integral part of the NDI’s mandate, a mandate regulated by the law it simultaneously enforces. While the ombudsman function resembles that of privacy advocates, with the need and ability to ‘generate politically relevant information’, arguably the NDI’s role as an administrative power makes it easier to ‘move it [information] by the most effective means to the place where it will have the most impact’ (Bennett 2008, 96).

Leverage politics

By ‘leveraging’ more powerful actors and institutions through material (money, goods, electoral votes) or moral (shame) leverage, ‘weak groups gain influence far beyond their ability to influence state practices directly’ (Keck and Sikkink 1998, 23). According to Bennett (2008, 123), privacy advocacy networks do ‘not have resources in the traditional sense’, but they do have a powerful issue. Hence, ‘the leverage politics of privacy advocacy is almost entirely about embarrassment, the loss of reputation, or what some commentators have called the “mobilization of shame” (Bennett 2008, 123)’. In contrast to conventional privacy advocates, the NDI is in a position of ‘decisionist’ power: it enforces data protection regulations and can sanction accordingly.²² However, we see that ‘leverage’ is a tactic employed by the NDI regarding issues that fall beyond the immediate interests, limits and relevance of privacy and data protection, and that are closer to what resembles engagement in political contestations and discourses.

Of particular concern is the security climate after 11 September 2001, which led to the predominance of security over privacy and other human rights issues. The war on terror receives considerable attention in the NDI’s reports, not only as regards illiberal security measures per se, but also as an instigating force for supranational discourses. In the immediate years following 2001, entire sections of the annual reports are dedicated to terrorism and organized crime, with particular attention being paid to the implications of counter-terrorism measures. However, around mid-decade, the NDI’s reports no longer include such specific sections; instead, the threats to privacy and data protection entailed in the war on terror are elevated into broader discourses on international cooperation, and particularly on issues relating to justice and policing. In consequence, a significant part of the NDI’s activities centers around participation in international forums on issues of privacy and data protection. Although these constitute arenas for information exchange, the NDI emphasizes that international forums are important for the influence they exert on relevant legislation as ‘with all due respect, it is the EU that today determines the shape of future norms and rules relating to data protection and information security’ (2007, 16).²³

²¹ In 2008, the NDI’s former director Georg Apenes received an award from both Computerworlds and the Norwegian Computer Society in recognition of his long-time work for the protection of privacy and personal data. In 2010, he was granted the Royal Norwegian Order of St. Olav, an order of merit for services to fatherland and humanity.

²² See Flaherty (1989) for a different view.

²³ According to the NDI, the Madrid bombings in 2004 gave further momentum to increasing the cooperation between police authorities within the EU (2005). With regard to the subsequent expansion of the Schengen Information System (SIS), the NDI cautions that, while its objective appears vague, the system will hold large amounts of information available for an increasing number of different authorities (2006). The expansion is a European agreement ‘on the stepping up of cross border cooperation, particularly to combat terrorism, cross border crime and illegal migration’, entailing an extensive intertwining of European databases filled with considerable amounts of personal data: DNA, fingerprints, and vehicle filing systems, to name but a few (NDI 2010). In addition, one may request further information from national authorities should one make a hit when searching the SIS. Thus EU member states may be granted permission to search databases containing extensive personal information concerning Norwegian citizens (NDI 2009).

International cooperation on security measures may reveal significant incoherence in data protection regulations, leading the NDI to warn against sharing data with countries that do not meet the demands of the EU regulations, and which the NDI has no influence over.²⁴ A recurring example has been US demands for extensive passenger list information from transatlantic flights, including those of Norwegian airlines. Although the European Data Protection Supervisor Peter Hustinx, has emphasized the importance of European and US willingness to compromise on the areas of privacy and data protection (Apenes 2005), the NDI (2004) claims that the US transfer of personal data is a clear breach of the core principles of European and Norwegian law (which is also an example of accountability politics, discussed next). In fact, the NDI presents the US as a particular concern in itself: initially it is somewhat wary of US actions, with this wariness increasing until the US and its security policies themselves are seen as posing threats to privacy and data protection. Evidence of this can be seen in the NDI's assertions that the US authorities have inspired those in Norway wishing to use the war on terror as excuse to collect and make use of more and more personal data (2004).

Accountability politics

Accountability politics describes attempts by advocacy networks to 'expose the distance between discourse and practice' (Keck and Sikkink 1998, 24) by holding those in power 'accountable to previously stated policies or commitments' (Bennett 2008, 96). Depending on the politico-legal context, private and public actors are held 'accountable' to public pronouncements and/or the law, such as the NDI statement concerning the transfer of personal data to the US.

However, in contrast again to privacy advocates, the NDI enforces law: holding private and public actors accountable under data protection law is an essential part of the NDI's *raison d'être*. Yet, as with how it practices leverage politics, the NDI engages in accountability politics on issues that are more general in scope than privacy and data protection, for instance human rights issues. One example concerns the 2002 immigration law amendments on expulsion and the use of immigrants' fingerprints in criminal investigations. Here the NDI writes that:

It may seem obvious that criminal immigrants should be deported, and that different crimes should be investigated by different means. But on what grounds and under which conditions should this happen? These questions should concern the legislator in a country that recently implemented the European Human Rights Convention. (NDI 2003, 20)

Symbolic politics

According to Bennett, privacy advocates conjure up familiar symbolic images as 'part of a process by which they may create awareness, solidify their networks, and expand the constituency of believers' (2008, 107). In their desire that 'powerful symbols' should become 'catalysts for change', privacy advocates frequently use well-known images such as 'Big Brother' to refer to 'virtually any over-intrusive surveillance scheme' (Bennett 2008, 107). In much the same way, the NDI invokes the concept of the 'Surveillance Society' throughout its reports, referring in particular to the images of totalitarian and disciplinary societies portrayed in Orwell's 'Big Brother' and Foucault's 'Panopticism'.²⁵

²⁴ Besides objecting to these developments on account of their consequences for privacy and data protection, the NDI also criticizes the processes whereby new regulations are made. For instance, the NDI criticizes the Prüm Convention - the expansion of the Schengen Agreement - for being neither sufficiently transparent nor democratic. The European Data Protection Supervisor was not properly consulted, and furthermore, because of Norway's relation to the EU, the Norwegian Data Inspectorate was unable to influence the legislation that is now becoming national law (NDI 2009). This kind of problem is a recurrent issue for the NDI: a democratic deficiency in the EEA agreement, arising from the discrepancy between inclusion in operational police cooperation and exclusion from full membership of the organizational bodies that serve to monitor this collaboration (NDI 2005).

²⁵ The linkages between the NDI's conceptions of surveillance and privacy discourses are, in fact, remarkably similar to the academic discourses within Surveillance Studies. Unfortunately, it is beyond the scope of this paper to explore this relation further.

In 2000, the NDI cautions that the ‘Surveillance Society’ is insinuating itself into our everyday lives, and it reiterates the same argument a decade later, claiming that a normalization of surveillance is transforming individuals into ‘obedient objects of surveillance’ (2009, 44). Much of the NDI’s concern relates to the subtle growth of monitoring and surveillance *without* democratic attention and debate: ‘it “invades” privacy and lacks democratic oversight or constraint, and leaves little or no room for political debate as to the consequences’ (Coleman 2011, 7). As an ombudsman for privacy and data protection defending its interests in grappling with new technological developments, the NDI identifies surveillance as an increasing threat to Norwegian society. The panoptic model of surveillance is a powerful metaphor in the NDI’s framing of contemporary surveillance threats. However, conscious of its limitations,²⁶ the NDI identifies trends in surveillance that go beyond the dichotomy of the watchers and the watched (2008).

Despite its clichéd quality, Bennett (2008, 107) points out that, for privacy advocates, ‘the symbol of 1984 continues to be used to connote excessive surveillance’. This seems very much to be the case for the NDI, who frequently refer to Orwellian surveillance in its reports; using either the original Big Brother metaphor for surveillance as a totalitarian practice of illiberal, bureaucratic states, or the altered and slightly expanded forms, such as the private-sector sibling Little Brother, or the ‘caring’ Big Mother. The latter signifies the expanding trajectory of care technology and surveillance, characterizing all the good helpers seeking to secure our health, economy, education and welfare—in exchange for a steady supply of considerable amounts of personal data, and access thereto (2008).

The most recent example of symbolic politics, however, is to be found in the high-profile debate on the implementation of the EU Data Retention Directive in Norwegian legislation. In a parallel to the way Keck and Sikkink (1998) see the catalytic role of the 1973 coup in Chile for the western human rights movement, resistance towards the EU Data Retention Directive by the NDI resembles the human rights strategy of expanding constituency by creating awareness and solidifying networks (Bennett 2008). Therefore, the next and final part of this paper will probe deeper into the role of the NDI in the DRD debate, paying particular attention to how the NDI manages its role in resistance as both an ombudsman and state administrative body.

Resisting the Data Retention Directive

In March 2006, the EU Parliament passed the Data Retention Directive 2006/24/EF, a framework for retaining telecommunications data from electronic mails and telephones in order to prevent terrorism and other serious crime. The content of communications may not be stored, but phone numbers and IP addresses as well as the time, length and physical location of those communicating may be retained for a minimum of 6 months to a maximum of 2 years. The EU/EEA member states are responsible for implementing the directive in their domestic legislations, including deciding the retention time, the definition of ‘serious crime’, and the appropriate authorities for retaining and managing the telecommunications data.

The EEA treaty gives Norway the right to veto EU directives, and although this option has never been taken, the controversial nature of the Data Retention Directive (from here on *directive*) led to considerable political debate among the Norwegian public. Two main rationales were cited in favor of adopting the directive. First, technological advances have affected the billing arrangements of telecommunications providers: as they are increasingly charging for *access to* rather than *use* of telecommunication services, they no longer need to retain data for billing purposes. As law enforcement agencies have enjoyed access

²⁶ The panoptic model has been criticized for being oppressive, directing attention towards certain characteristics of surveillance while ignoring others (Haggerty 2006).

to these data, under certain regulations,²⁷ the changes in billing arrangements will consequently deprive law enforcement agencies of this information. This loss has come to seem all the more important because of the second rationale, namely the significance of this data for the detection, investigation, and prosecution of serious crime, although practitioners and scholars alike have hotly disputed this (see Vorrat 2011; Feiler 2010). Nonetheless, the political climate after the Madrid and London bombings in 2004 and 2005 facilitated, or even required, assertive security measures such as the DRD (Feiler 2010).

Thus, it is not surprising to find that those who favored the implementation of the directive in the Norwegian debate were predominantly representatives of law enforcement and justice agencies. The police, the National Authority for Prosecution, the Norwegian Police Security Service and KRIPOS, a special police division concerned with serious and organized crime, all endorsed the directive on the ground that it is essential to the fight against serious crime, and especially the fight against terrorism and child pornography. Failure to implement the directive was cast as an impediment to international police and security cooperation, with the ultimate consequence that Norway would become an international ‘free haven’ for serious crime.²⁸

The NDI, on the other hand, has been a firm opponent of the directive from the start; even when the directive was nothing more than an EU ambition to establish a joint regulatory framework, the NDI strongly resisted the development in its annual reports. When the directive came into force in 2006, they began treating the issue separately and with great concern, warning that it constituted a ‘paradigm shift’ in the Norwegian justice system by undermining the presumption of innocence, a fundamental cornerstone of the liberal constitutional state (2007, 31). It has been characterized as a completely new tool for the government to subject the entirety of its citizens to large-scale surveillance and control (2007, 31), and the NDI’s former director, Georg Apenes, referred to it not only as a ‘major breach of the traditional principles of law’ but also as an indication of a ‘totalitarian infatuation’ (Hammerlin 2010, 47). Informing the public of the directive’s implications has thus been made a priority by the NDI, and to this end its representatives have made frequent appearances in public debates, held lectures and written commentaries in the media as well as engaged in social networking on Facebook and Twitter (NDI 2009).

The NDI played a key role in what would become a widespread resistance network against the directive, drawing on its role as ombudsman and on ‘expert opinion’ to mobilize resistance ‘by identifying and providing convincing explanations for powerful symbolic events, which in turn become catalysts for the growth of networks’ (Keck and Sikkink 1998, 22). Mobilizing in the summer months of 2008, the public discourse was characterized for more than two years by public debates and organized resistance—among academics, activists, journalists, politicians, and technologists alike—with numerous editorials and readers’ letters, articles and blogs, and not least public demonstrations and cross party ad hoc organizations opposing the directive.²⁹ This being so, the debate may have led to a shift in the political awareness of a wider audience, moving beyond the traditional fault lines of EU membership disputes. The public debate can therefore hardly be seen as anything other than a success in the eyes of the NDI, since it finally brought the attention of the public to the issues of privacy and data protection. Former Supreme Court Judge and privacy activist Ketil Lund has gone as far as to characterize the debate as the most significant event for the interests of privacy and data protection in a very long time (2010).

According to Peter Hustinx, political decisions that weaken privacy and data protection are accepted insofar as their consequences affect distant peoples and populations. If the values ensuring people’s safety

²⁷ Their access is regulated inter alia by the Norwegian Post and Telecommunications Authority.

²⁸ These arguments are collected from the written submissions on the directive from relevant organizations.

²⁹ *Stop datalagringsdirektivet* is the name of a cross-party organization established for the sole purpose of fighting the implementation of the directive in Norwegian law; see <http://www.stopdld.no>. In addition, an on-line petition against the directive, initiated by the blogger Vox Populi, mobilized over 18,000 signatures.

and well-being are threatened, he claims the outcome will be public outrage (Apenes 2005). Yet, as is pointed out by Aas et al. (2009, 1), the reception given to different security measures may be equally dependent on the *possibilities* of resistance; they note that ‘not all social groups are equally willing to accept that they are put under suspicion, nor do they have equal possibilities of resistance’. Reflecting Bennett’s (2008, 94) mapping of the ‘privacy advocate’, the individuals, groups and organizations involved in the resistance were from various backgrounds, though ‘[m]ost have higher levels of education’ and ‘[a]ll have deep-seated worries about the abuses of power by modern organizations using the latest technological tools’. Particularly visible, after the NDI and politicians, was the legal community, spearheaded by ‘liberal activists’ such as the before-mentioned Ketil Lund, and Jon Wessel-Aas, head of the Norwegian section of the International Commission of Jurists. Large segments of the media were also opposed to the implementation of the directive, arguing that it would undermine their ability to provide sources with protection, and that in these times of (wiki)leaks, it would silence whistle-blowers (Jørgenrud 2011).

Although raising awareness of what was at stake, the high-profile resistance did not succeed in preventing the directive’s introduction into Norwegian law altogether, but did most likely cause a significant delay in its progress through parliament: originally scheduled for 2009, the directive was not passed in parliament until 2011.³⁰ Nonetheless, in the run-up to the 2011 parliamentary reading, the debate peaked. Although not part of the coalition government, the Conservative Party, struggling to reconcile their EU fervor with the values of conservative liberalism became crucial to the outcome in parliament. In the end, the directive was passed on 4 April 2011, with 89 votes to 80.

In spite of the failure to prevent the implementation of the directive in Norwegian law, the widespread public resistance and the debate it generated was a success for the NDI in terms of raising awareness and interest in privacy and data protection issues. However, less than two months before the directive was passed in parliament, the NDI launched what was referred to as a compromise in the Norwegian newspaper *Aftenposten*. Instead of implementing the directive as a whole, the NDI argued for the extended retention of IP addresses to meet the needs of law enforcement agencies. In the light of the NDI’s hitherto public resistance, this sudden move appeared incomprehensible to those following the debate. At the very least, it raises interesting questions regarding the NDI’s institutional self-image regarding its power/position to offer/enact political compromises; two possible explanations of this will now be given.

First, even though the PDA defines IP addresses as personal data, the NDI regards their retention as the least intrusive of the measures sought in the directive. As its director proclaimed, ‘[t]here is an essential difference between identifying the persons behind IP addresses and a total mapping of who is talking to whom, and when and where the individual citizen is physically located’ (Nationen 2011). Here it is not the war on terror that is emphasized but rather the fight against child pornography, a crime that is almost exclusively carried out on the web.³¹ Nevertheless, in terms of the before-mentioned precautionary trend in criminal justice, the NDI appears to abandon its principled stand on privacy-infringing measures in anticipation of wrongdoing—terror related or not.

Second, in 2010 the NDI’s long-standing director Georg Apenes retired and was replaced by Bjørn Erik Thon,³² who came from the directorship of the Norwegian Consumer Ombudsman. He is considerably younger than Apenes, although they share the same legal background and political roots in liberalism.

³⁰ The directive came into force on 1 July 2012.

³¹ The emphasis on online child pornography rather than on terrorism may be explained by the fact that the former is less politically ‘challenging’ in the Norwegian populace than the implementation of supranational counter-terrorist measures, albeit this was prior to Norway’s own experience of terror: on 22 July 2011 the government buildings were bombed in central Oslo followed by a massacre at the political youth camp of Utøya.

³² Ove Skåra was acting director in April–May before Bjørn Erik Thon was formally in place.

Thus, the so-called compromise can be interpreted as a result of this new leadership: a high-profile case enabling Thon not only to stake out a new course for the NDI, but also to position himself within this landscape. His was a more pragmatic and less principled stance, balancing the interests of privacy and data protection with other societal needs, such as security. In the light of constant questions concerning whether or not the NDI is able to take such considerations into account—questions arising from its dual nature—Thon might well have taken the opportunity to reduce this tension. The significance of the NDI leadership change is also reflected in Apenes' response: as the spokesperson for a newly established non-governmental privacy network, *Digitalt Personvern* [Digital Data Protection], whose aim is to put the directive on trial, he said 'we are not open to compromises' concerning the directive (Christensen 2011).

Conclusion

The delineation of the debate on the EU Data Retention Directive in Norway and the role the Norwegian Data Inspectorate has played in this drama illustrates the inherent tension stemming from its institutional twofold function. Prior to the 'compromise', the NDI was firm in its resistance, carrying out its role as ombudsman to the highest degree, by protecting the interests of privacy and data protection and at the same time strengthening this resistance through network-building of what would become new privacy advocates. The NDI's new leadership appears to be charting a new course, partly as a result of previous criticism concerning the balance of not only the two functions of the NDI but also the interests of privacy and data protection vis-à-vis other societal values. Hence, the 'compromise' represents an attempt to reduce the NDI's institutional complexities. However, this practical move may prove to weaken the NDI's role in resistance; traditionally, it is its principled posture that has been its forte, albeit a contested one. It is not the role of a watchdog to please for the sake of pleasing.

The review of strategies of persuasion, comparing the NDI's practices with the tactics employed by privacy advocates in particular and transnational advocacy networks in general, reveals that the NDI is far from an ordinary privacy advocate. Rather than resembling privacy advocates, the NDI picks its tactics as it sees fit, and especially, it seems, when pursuing a politico-normative argument beyond the immediate issue of privacy and data protection, engaging in broader political debates in the public discourse. This has made the NDI an important opinion-former throughout the past decade: a position that is at the same time produced and revealed by the institutional tensions from its roles as a privacy-advocating ombudsman and an administrative supervisory body.

Acknowledgements

The Norwegian Research Council as part of SORISK-UP, under the SAMRISK program, financed the research for this paper. The author is sincerely grateful to Katja Franko Aas, J. Peter Burgess, Mareile Kaufmann, and Kristin Bergtora Sandvik for their generous comments on earlier drafts, and Georg Apenes and Thomas Mathiesen for sharing valuable insights with the author.

References

- Aas, Katja Franko, Helene I. Gundhus, and Heidi Mork Lomell. 2009. *Technologies of inSecurity: the surveillance of everyday life*. Abingdon: Routledge-Cavendish.
- Apenes, Georg. 2005. *Fra tillit til kontroll: Tolv samtaler om politikk, teknologi og personvern*. Oslo: Pax Forlag A/S.
- Bennett, Colin J. 2008. *The privacy advocates: resisting the spread of surveillance*. Cambridge: The MIT Press.
- Boe, Erik. 1993. *Statsrett og forvaltningsrett*. Vol. 2, *Innføring i juss*. Oslo: TANO.
- Christensen, Kenneth. 2011. Inngår ingen DLD-kompromisser. *Computerworld*, 18 October.
- Christensen, Tom, Morten Egeberg, Helge O. Larsen, and Paul G. Roness. 2002. *Forvaltning og politikk*. Oslo: Universitetsforlaget.
- Coleman, Roy. 2011. *Surveillance and crime*. Los Angeles: Sage.
- Difi. 2011. Evaluering av Datatilsynet. In *Rapport 2011:8*: Difi.
- Feiler, Lukas. 2010. The Legality of the Data Retention Directive in Light of the Fundamental Right to Privacy and Data Protection. *European Journal of Law & Technology* 1.
- Fernandez, Luis A., and Laura Huey. 2009. Is Resistance Futile? Thoughts on Resisting Surveillance. *Surveillance & Society* 6 (3):199-202.

- Flaherty, David H. 1989. *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.
- Haggerty, Kevin D. 2006. Tear down the walls: on demolishing the panopticon. In *Theorizing Surveillance: The panopticon and beyond*, edited by David Lyon. Cullompton: Willian.
- Hammerlin, Joakim Wigdahl. 2010. *Terrorindustrien*. Oslo: Manifest forlag.
- Introna, Lucas D., and Amy Gibbons. 2009. Networks and Resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance & Society* 6 (3):233-258.
- Jørgenrud, Marius. 2011. DLD - et våpen mot varslere. *digi.no - IKT bransjens nettavis*, <http://www.digi.no/866306/dld-et-vaapen-mot-varslere>.
- Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists beyond borders: advocacy networks in international politics*. Ithaca, NY: Cornell University Press.
- Kjeldstadli, Knut. 1999. *Fortida er ikke hva den en gang var : en innføring i historiefaget*. Oslo: Universitetsforlaget.
- Lund, Ketil. 2010. Nedbyggingen av den liberale rettsstat. In *Til forsvar for personvernet*, edited by Kristin Clemet and John O. Egeland. Oslo: Universitetsforlaget.
- Lyon, David. 2006. *Theorizing surveillance: the panopticon and beyond*. Cullompton: Willan.
- Marks, Peter. 2002. Imagining surveillance: Utopian visions and surveillance studies. *Surveillance & Society* 3 (2/3).
- Martin, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6 (3):213-232.
- Marx, Gary T. 2009. A Tack in the Shoe and Taking off the Shoe Neutralization and Counter-neutralization Dynamics. *Surveillance & Society* 6 (3):294-306.
- Melton, Gary B. 1991. Lessons from Norway: The Children's Ombudsman as a Voice for Children. *Case Western Reserve Journal of International Law* 23: 197-255.
- Nationen. 2011. Datatilsynet foreslår datalagringskompromiss. *Nationen*, 7 February.
- NDI. 2001. Datatilsynets årsmelding for 2000. edited by Arbeids- og administrasjonsdepartementet. Oslo: Arbeids- og administrasjonsdepartementet.
- . 2002. Datatilsynets og Personvernemndas årsmeldinger for 2001. edited by Arbeids- og administrasjonsdepartementet. Oslo: Arbeids- og administrasjonsdepartementet.
- . 2003. Datatilsynets og Personvernemndas årsmeldinger for 2002. edited by Arbeids- og administrasjonsdepartementet. Oslo: Arbeids- og administrasjonsdepartementet.
- . 2004. Datatilsynets og Personvernemndas årsmeldinger for 2003. edited by Arbeids- og administrasjonsdepartementet. Oslo: Arbeids- og administrasjonsdepartementet.
- . 2005. Datatilsynets og Personvernemndas årsmeldinger for 2004. edited by Moderniseringsdepartementet. Oslo: Moderniseringsdepartementet.
- . 2006. Datatilsynets og Personvernemndas årsmeldinger for 2005. edited by Fornyings- og administrasjonsdepartementet. Oslo: Fornyings- og administrasjonsdepartementet.
- . 2007. Datatilsynets og Personvernemndas årsmeldinger for 2006. edited by Fornyings- og administrasjonsdepartementet. Oslo: Fornyings- og administrasjonsdepartementet.
- . 2008. Datatilsynets og Personvernemndas årsmeldinger for 2007. edited by Fornyings- og administrasjonsdepartementet. Oslo: Fornyings- og administrasjonsdepartementet.
- . 2009. Datatilsynets og Personvernemndas årsmeldinger for 2008. edited by Fornyings- og administrasjonsdepartementet. Oslo: Fornyings- og administrasjonsdepartementet.
- . 2010. Datatilsynets og Personvernemndas årsmeldinger for 2009. edited by Fornyings- administrasjons- og kirkedepartementet. Oslo: Fornyings-, administrasjons- og kirkedepartementet.
- . 2011a. Datatilsynets strategi 2011-2016. Datatilsynet.
- . 2011b. Datatilsynets årsmelding for 2010. Oslo: Datatilsynet.
- NOU 2009:1. 2009. Individ og integritet: Personvern i det digitale samfunnet: Utredning fra Personvernkommisjonen oppnevnt ved kongelig resolusjon 25. mai 2007. edited by Fornyings- og administrasjonsdepartementet. Oslo: Statens forvaltningstjeneste.
- Personal Data Act. 2000. Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act).
- Personal Health Data Filing System Act. 2001. Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act).
- Power, Michael. 1997. *The audit society: rituals of verification*. Oxford: Oxford University Press.
- Schartum, Dag Wiese. 2008. Designing and Formulating Data Protection Laws. *International Journal of Law and Information Technology* 18 (1):1-27.
- Stub, Marius. 2010. *Tilsynsforvaltningens kontrollvirksomhet: undersøkelse og beslag i feltet mellom forvaltningsprosess og straffeprosess*, Det juridiske fakultet, Universitetet i Oslo, Oslo.
- Vorrat, AK. 2011. Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics. AK Vorrat.