Communicating Privacy in Organisations. Catharsis and Change in the Case of the Deutsche Bahn

Manuscript for submission to CPDP 2012 edited volume

Daniel Guagnin, Carla Ilten, Leon Hempel

Abstract

The main challenge in implementing privacy and data protection in organisations is bridging the gap between law and practice. Most data controllers feel little incentive to put effort into this demanding process of translation from rule to action. We present an analysis of the fundamental transformation of the Deutsche Bahn corporation (DB) with regard to privacy and data protection policy and implementation. We argue that the scandal-afflicted organisation has started approaching data protection implementation as a problem of *communication* and *negotiation*. In full acknowledgement that insecurities exist and will always emerge as a function of business activities and technological changes, the goal of the DB's data protection officers is not to end up with a static set of rules and responsibilities, but to rebuild trust within the organisation and find ways to deal with insecurities in the future - openly and flexibly and in close dialogue with managers, employees, their representatives and the data protection authorities. The case thus exemplifies the role of communication in bridging the gap between law and practice.

1. Introduction

This contribution presents an analysis of the fundamental transformation of the Deutsche Bahn corporation (DB) with regard to privacy and data protection policy and implementation. We will argue that the scandal-afflicted organisation has started approaching data protection implementation as a problem of *communication* and *negotiation*. Its development shows first successes in regaining trust and improving protection through massive efforts to translate data protection law into day-to-day privacy aware practices.

The case study[1] has been conducted in the framework of the EU-project "Privacy Awareness through Security Organisation Branding". The project performed an analysis of privacy awareness in security-related organisations and of their security and privacy communication in

1 The present case study is a composite analysis from a number of activities - both structured and informal - over the course of the PATS project (2009-2012). In detail, it is based on conversations between the authors and Data Protection Authorities as well as privacy activists who were involved in the present case as well as conversations conducted with DB staff in different contexts; more supporting material was acquired through own online research and media analysis. The analysis must not be read as a definitive representation of the current situation at the Deutsche Bahn, but should be understood as a case-inspired conceptual contribution.

six countries[2]. One important insight from the interview processes is that a paralysing silence governs security markets when it comes to privacy protection. While actors acknowledge that it is a challenge to translate data protection law into practice, they have no incentives to become more active about these problems.[3]

Building on PATS's initial assumption that self-regulation in this field could be fuelled by communication - more specifically, "branding" as an act of self-presentation and improvement - we inquired about the possibility of more public communication by these companies. This concept of a proactive, ongoing effort by data controllers to manifest their compliance is akin to the rekindled discourse around accountability.[4]

In line with the accountability idea and linked discussions, we have argued that privacy protection needs to become a reflexive ongoing process within the data controlling organisation. This self-critical process is the basis for an increasing awareness about privacy issues and the starting point for implementing effective structures of accountability to ensure good privacy practices. What the project initially targeted with the use of the term "branding" can be understood as a complex of communication, both within organisations and into society[5].

The case of the Deutsche Bahn exemplifies the role of communication in bridging the gap between law and practice. The corporation underwent massive scandal due to the surveillance of employees well into their private lives on a systematic basis. After experiencing complete image calamity, the organisation implemented a potent data protection infrastructure whose primary asset is (wo)manpower: over the course of an entire year, employee and employer representatives, board members and personnel managers were involved in negotiating the new DB privacy and data protection policies. In this process, a new organisational data protection infrastructure has been created. Another year saw an extensive process employee training and communicating the achievements to the workforce. What is more, new approaches to dealing with the translation of policies into practice are experimented with. Again, these consist mainly of communication on an ongoing basis in a trusting atmosphere between workforce and data protection officers, as we will show.

---

2 PATS partners include the UK, Israel, US, Poland, Finland, and Germany. The project is funded under the EU FP7. Further information and related reports and publications can be found on www.pats-project.eu.

3 Cf. Carla Ilten et al., "How Can Privacy Accountability Become Part of Business Process?" *Privacy Laws and Business International*, no. 112 (September 2011): 28-20.

4 Recent contributions to the accountability discourse can be found in the book "Managing Privacy through Accountability", ed. Daniel Guagnin et al. (Palgrave Macmillan, 2012 forthcoming): Joseph Alhadeff et al., "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions."; Colin Bennett, "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats.". From the European Commission see "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A Comprehensive Approach on Personal Data Protection in the European Union." (2010) and Article 29 Working Party. "Opinion 3/2010 on the Principle of Accountability", (2010). The debate is also outlined in Daniel Guagnin et al., "Privacy Practices and the Claim for Accountability." In *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, ed. René Von Schomberg. (Luxembourg: Publication Office of the European Union, 2011).

5 On the basis of our results, we have developed a privacy branding model which you can find in detail at the project website pats-project.eu, see also Daniel Guagnin et al.. "Bridging the Gap: We Need to Get Together." In *Managing Privacy Through Accountability*, ed. Daniel Guagnin et al. (Palgrave Macmillan, 2012).

2. Scandal

Even though it is likely known to the reader what happened at the Deutsche Bahn, we will briefly sketch the story of one of the biggest scandals revolving around privacy infringement and data protection failure.

In 2009, it became public that employees - hundreds and thousands of them - had been surveilled and researched by external agencies, Network Deutschland GmbH in particular, by order of DB staff. Over the course of months, more and more details about the extent of the spying and data exchange came to light: not only employees, but their spouses as well had been investigated with regard to their private finances including money transfers, travels, online behaviour, and biographical data, among others. The orders to establish these data have been given orally by DB members in charge of "fighting corruption", and sums as large as € 800.000 were agreed on without formal documentation.

The surveillance affected all levels of employees - works council members as well as managers. The substance of the infringing activities makes this a real privacy issue – not just one of careless data loss. While data protection is often equated with data security, this case reminds us that privacy starts with the non-existence of data rather than their protection. The private lives of employees have been illegally intruded for purposes of control and internal policing, over the course of years. [6]

Such systematic surveillance is not the failure of an individual. Rather, an entire network within the corporation was involved in this attempt at managing the DB through finding its "black sheep" - critics of the stock launch so fervently put forward by CEO Hartmut Mehdorn, for example, who were suspected of handing information to the media. In a sense, Mehdorn and those engaging in the surveillance activities were trying to control the information flow about the corporation by controlling employees.

Needless to say, the DB data protection scandal caused a complete loss of trust among the majority of the workforce as well as a good measure of anger. The atmosphere was more than stormy - something drastic needed to happen in order to create clean air.

3. Catharsis

As we have observed in the PATS interviews on privacy awareness in the security field, companies find different answers to dealing with scandal. Companies can react with retreat, or they can emerge and attempt to re-cast their image. With regard to the public, this seems to be a fight-or-flight decision for organisations - depending on what is at risk or can be gained in the situation.

Obviously, a scandal of the scope as described for the DB is nothing that can be pushed aside easily. The scandal and CEO Mehdorn's personal involvement kept the media busy for months. The criminal espionage activities concerned the workforce, which means that next to the public and stakeholders, the very base of a fairly traditional organisation had lost their trust in the

6 For a discussion of how privacy and data protection are differently legally defined see Rapha・ Gellert and Serge Gutwirth, "Beyond Accountability, the Return to Privacy?" In *Managing Privacy through Accountability*, ed. by Daniel Guagnin et al. (Palgrave Macmillan, 2012).

company and demanded consequences.

Secondly, the activities were closely tied to the politics of the DB future development and Mehdorn's iron vision of a stock-noted corporation. The scandal seemed to be born out of an authoritative style of management, and nothing about it was negligible or laissez-faire. In addition to the surveillance of workforce, a related affair of media manipulation with regard to the issue of a possible stock market launch and to union strikes became public.

Real personnel consequences were imperative. CEO Mehdorn, a powerful and adamant leader, had to offer his resignation in March 2009. The new CEO Rüdiger Grube consequently exchanged most of the top management, who proved to be intensely involved in the affair. The representatives of corporate security, auditing, and anti-corruption had to leave. Massive organisational restructuring followed, including the creation of a Board-level Department for Compliance, Legal, Data Privacy and Security which also hosts the new data protection officer, as we will lay out in detail below.

Lastly, a monetary penalty was imposed on the DB through the Berlin state data protection officer, Alexander Dix. It was the largest sum ever inflicted in the legal area of data protection in Germany - over €1.1 million, which were paid by the DB without objection.

As a corporation of public interest - being the railway provider and completely state owned - catharsis needed to happen for the DB in order to become worthy of the trust of both the public, policy makers, clients, and most of all, its employees. The act of renewal of the top management was an important instance of "purging" the responsible actors, preparing the ground for change. As in Greek drama, the public took part in this catharsis as an audience which was delivered shameful news on a daily basis - the loss of privacy became public, palpable for everyone. Outrage and punishment made for relatively clean air after the foul weather.

4. Change: "A new era"

While catharsis is strongly connected to symbolic events and public communication, real organisational change takes place not only in structures, but in the knowledge, attitudes and everyday activities of employees. In conversations about the DB case, there is a clear before-and-after rhetoric with regard to catharsis: a new era has begun.

In the case of the DB, scandal affected employees' trust in the corporation in particular since the spying was directed at workforce, who demanded change vocally - an internal problem. Accordingly, catharsis needed to be communicated both outwards and inwards by the organisation.

The following process of change that will be described now is a slow and profound one; it is about regaining trust and including as many actors as possible. It is about communicating privacy. We will first describe the formation of the corporate works agreement, which itself is the outcome of a yearlong process of communication within the DB. Next, we will reproduce how this agreement was communicated to all members of the DB.

4.1 The Corporate Works Agreement

4.1.1 Negotiating the agreement – an act of communication

The Corporate Works Agreement ("Konzernbetriebsvereinbarung" , KBV) is the outcome of one year of negotiation between representatives of different levels of the DB and has been adopted in November 2010. After the 2009 data protection affair had revealed all the details of employee surveillance and spying practices, a "poisoned atmosphere" impregnated the whole corporation. Initially, a lot of tension was felt in the discussions and negotiations about how to put new data protection mechanisms in place. It was even a challenge to find common language for a mutual understanding. The KBV was mainly negotiated by a working committee called "Employee Data Protection" which incorporated representatives of employers and employees, the central works council, the human resources department, subsidiaries and the data protection office.

The whole process of negotiation was essential for regaining the trust of the employees. Thus the negotiations themselves were a process of building mutual understanding and communication. The fact that the KBV was completed in this way led to appreciation on the part of employees - after all the unpleasantness, something was happening. The data protection office made a point of actively communicating that data protection is not only about protecting bits and bytes but about human beings. In other words, privacy is not only about secure data storage and transfer but first of all restricting the data sets about human beings (principle of data economy). This message was addressed to employer stakeholders especially. The active communication of these concepts can be understood as a measure of awareness building.

4.1.2 Beyond law, towards accountability

Since the KBV was developed in the dire need of regaining trust and was negotiated by different stakeholders, the outcome is far beyond simple compliance with data protection law. While the agreement is naturally based on legal frameworks, it has in fact a progressive character and anticipates potential changes imminent with the amendment of German data protection law which is ongoing. Moreover, the agreement may even provide an example for solutions with regard to the claim for accountability which has regained importance over the past years.

The agreement can be understood as a reflexive definition of the future data protection practice of the Deutsche Bahn. It is a prospective declaration; a manifest of how privacy practices shall be organised and implemented.[7] The next section will shortly outline the structural changes in the organisation of data protection which are initiated by this agreement.

4.2. New actors and structures - implementing accountability

In this part, we will outline the structural changes that have been made with regard to data protection at the DB. To contrast the restructuring with the earlier set-up, we will firstly sketch the structure before the éclat in 2009.

---

7 The Corporate Works Agreement "Employee Data Protection" can be downloaded at http://recht.verdi.de/beschaeftigtendatenschutz/data/Konzernbetriebsvereinbarung.pdf (German) [last accessed 1.3.2012]

A central data protection office was in place for the whole group with one Group Data Protection Officer (GDPO) and five assistants. Besides, there were about seventy "contact persons" in the different business areas, especially in business areas where data protection was of high relevance. For these contact persons, data protection activities were an addition to their normal tasks. They were trained internally and their main function with regard to data protection was to be a contact person for the GDPO - not the data processing employees. In practice, they had relatively little data protection expertise and were hardly involved in discussions about changing processes and procedures in the different business areas. Instead, the GDPO negotiated issues with the management of the respective business areas, and the "contact persons" were informed after the fact.

A few more random DPOs existed at some of the DB group companies. However there was no real framework for interaction between these different data protection instances. In this set-up, the officers were not entirely independent. Tellingly, a substantial overview of the DPOs in place was only gained in the process of restructuring. Seen that this represents the entire organisational structure of privacy and data protection for a corporation with a +200.000 workforce, the status of data protection before 2009 is clear. The lack of elaboration, independence, and interaction between data protection bodies shows that it was not considered a significant issue by the management.

When the working committee "employee data protection" was installed, they realized that they would have to define new and more effective organisational structures. A first challenge was finding the adequate number of people in charge of data protection. On the one hand, the first goal was to provide the employees the best support possible, on the other hand the corporate structure of the DB needed to be integrated in order to keep the office visible and manageable. While a great number of new data protection experts were installed, their distribution and number needed to be balanced carefully - especially with respect to an easy mutual communication between the representatives and a common understanding.

The first action to strengthen the organisational data protection structure at the DB was to enhance the top level group data protection office. The office, headed by the GDPO Ms Newiger, got five departements with dedicated functions: Client and employee data protection got one department each, additionally one department for audits have been set up and two departments for the management of the decentralized data protection structure of the whole group, split into business areas.The GDPO is responsible for the group and subsidiaries except for five more DPOs which are assigned to subsidiaries.[8] All the DPOs are independent and instruction-free from the management or other levels of organisation. This line of six DPOs is the top level of full-time independent DPOs.

The DPOs' competences include controlling the correct processing and application of personal data software, ensuring that employees processing personal data are adequately trained for compliance with the legal provisions; and evaluating automatic data processing systems with regard to whether they constitute a risk to the rights of the concerned data subjects.

Next to the top level, it was deemed important to install a secondary structure of trained assistants which operate in the several business areas of the corporation. At this next level, ten highly skilled "Trained Assistants for DP" have been introduced whose competences are

8 See http://recht.verdi.de/beschaeftigtendatenschutz/data/Konzernbetriebsvereinbarung.pdf

comparable to the DPOs. They receive the same training and are dedicated to DP tasks full-time. Their assignment relates to the specific DP issues of their business area. In their function of DP Assistant, they are granted a special employment protection which exceeds the end of their activities as DP Assistant by a year. The assistants are instructed by and regularly meet up with the central data protection office, and are legally part of the subsidiary they are employed in.

In addition to the levels Group DPO, DPOs and Assistants, another category of "Data Protection Confidants" has been created. Data Protection Confidants are instructed by the Trained Assistants for DP. They may be assigned other duties besides their Data Protection tasks, but it is defined that their tasks related to Data Protection issues are first priority. The Data Protection Confidants report to the Trained Assistants and are charged with conducting monitoring in their Business Areas, as well as with giving feedback to the Group DPO and the corporate management and to report Data Protection violations.

In all, there are currently more than a hundred Data Protection Confidants assigned to represent the Data Protection Office broadly in the whole national DB group corporation. The time split between Data Protection and other tasks is a challenging question and the Corporate Works Agreement offers definitions that help employees dedicating enough time to these purposes. Models for calculating the exact amount have been discussed. It is generally agreed that work in committees, trainings, travels and similar educational time uses are a necessary part of this assignment.

All employees charged with Data Protection tasks on all levels enjoy the training by the German Association for Data Protection and Data Security (GDD) who provides official certification. The GDD is an independent association which builds expertise and provides training and other services with regard to data protection. It is highly recognized by the authorities and proved to be the only organisation capable of handling the mass demand for trainings in such a short time frame for the DB. A total of about 150 employees has been trained until now.

The dimensioning of the data protection infrastructure will be tested over the next years and revised if needed. The current situation thus represents the first approach by the Data Protection Working Group. While there are calls for a "return on investment" by some management actors, it is generally expected that the basic new structure of DPOs and Trained Assistants will be preserved in any case.

To sum up, the restructuring of the organisational structure and competences must be evaluated as a giant leap in terms of both numbers and quality. The new infrastructure comes as a huge investment and is extremely visible both within the company and to the public.

Next to building these structures in working groups and through the collective process of creating the KBV, the most important step in regaining trust within the company was to communicate these changes to the workforce at large. In the case of the DB, creating and communicating the changes went hand in hand. Translating the formal rules into practice has become pretty much a public affair within the DB, as the following section will outline.

4.3. Spreading the news: communication

The training of the data protection officers, trained assistants and confidants was a considerable instance of communication, a process which started in March 2011 and is nearly finished. In the

direction of the workforce, a communication concept which aims at spreading the message about the new era of data protection in detail has been devised. It was understood that the new KBV would unfold the greatest impact if the changes and the progress made were understood by all employees.

The first step in this process of communication was to conduct six regional conferences with about 3000 attendees. Executives, stakeholders, personnel managers and data protection representatives were invited. The management board was present with one or two representatives, and chairpersons of the trade unions and working council attended. Due to the kick-off meeting character of the conferences, it was not possible to address all questions, rather the event conveyed the general turn of the DB data protection policy. Among the employees, a high demand for participation was reported.

Consequently, smaller regional workshops with about 30 attendees were conducted by the human resources department, the trade union and the central data protection office. There, after a short presentation of the data protection policies and the Corporate Works Agreement, the attendees were split into groups to collect questions and concerns which were then discussed in one day workshops. In this context employees had the opportunity to find out what the KBV means in the very practice of everyday activities.

The DB has an infrastructure of regional networks in place where personnel managers of the different business areas in each region meet to balance their interests for a joint go ahead. These networks have been used by the central data protection office to spread the changes to the business areas. This way, the personnel staff could discuss their questions and concerns in a confidential sphere, and dialogue between different stakeholders (working council, unions, and management personnel) was opened up.

The regional workshops were met with large demand as well. In 2011 all workshops were booked out and follow-up workshops are planned for 2012. The feedback from the workshops was quite positive, criticism is mostly voiced about the practice relevance of the instruction material. The translation between theory and practice is still difficult and leaves attendees stating that a follow-up seminar with more example cases would be welcomed. This shows the importance of Data Protection staff - rather than policy texts - within the organisation. People need contact persons to discuss their practice cases. A single document such as the KBV is an important milestone, but does not accomplish the translation into practice by itself. Structures of accountability need to be defined, but these structures need to enable continuous communication to take effect in organisational practice.

For the DB change process, this means that after the phase of creating the new data protection infrastructures, the continuation of communicating privacy needs to be organised. To this end, data protection jour fixes are installed where every 2 months data protection representatives of all levels come together to discuss standards and upcoming issues. These meetings are intended to stimulate communication between the data protection representatives and at the same time support the diffusion of data protection related issues to the work force. This process of dissemination is still unfolding.

Beyond these events of personal communication, broadcast communication has been set up through an online information platform on the DB Intranet. Supporting guidelines have been published in print. The internal print media are also used to communicate the changes achieved

through the KBV. Step by step, the new data protection policy is presented and translated for the workforce.

On a more general level, the DB has set up an accessible procedure for whistle-blowing in all compliance matters. This includes privacy and data protection issues and is a measure of empowerment for the workforce.

While there are no official or formal tools that are used for measuring the effect of communication on trust or the general atmosphere among the employees, the many communication events lead to a fairly good sense of "atmosphere" for the data protection representatives involved.

5. New experiences: bridging the gap

The above-described intense measures of communication and the related employees' reactions provide us with valuable insights into the difficulties of bridging the gap between law and practice. Data protection regulation is a legal area that comes with some latitude. There is black and white, but only rarely - between them lies the margin of discretion - which has been narrowed the KBV, but still it takes an individual case assessment most of the time.

It is this process of *translation* from rule to action, as we have called it elsewhere[9], that makes privacy and data protection so complex. There is no denying that in order to implement data protection effectively, resources need to be dedicated. What these resources consist of, though, is a concept that is changing: the translation of law into practice calls for human translators who provide support on an ongoing basis. The problematique of data processing inside and outside of standard systems in a large organisation exemplifies this line of thought.

5.1 Data within and outside of "IT standard systems" [10]

In a large corporation like DB, IT systems are fairly standardised and well-defined, but with the same token also limited. In general, these kinds of configuration lead people to start operating outside the standard system for simple purposes. Operating outside standard IT systems, though, means that all security and data protection standards devised for the standard systems will also be circumvented. The mere set up of a simple Excel table for the purposes of making a list of participants for an event could legally become a matter of consent through the works council when it is done outside of standard systems of data processing[11] - a rule that can become highly hindering in many everyday situations that seem innocuous.

Simply circumventing rules, however, re-creates the well-known gap between law and practice. If rules were to be implemented perfectly, all processes would be defined. In the described situations of conflict, it means that processes that move at the margins of these rules and are not yet defined *within* them either need to be carried out in secret - or become (re-)defined.

---

9 Guagnin et al, "Bridging the gap " op. cit.

10 This section reflects on § 9 of the Corporate Works Agreement, "Nebendatenverarbeitung"

11 cf. § 9 of the Corporate Works Agreement, op. cit.

In conversations we had about this topic, the complexities and difficulties of putting data protection law into practice in everyday business going on were acknowledged within the DB. Compared to our earlier research on privacy awareness in security-related companies, this is a massive step forward from a dead quiet to an acknowledgement.

If a procedure is sufficiently desirable to be included in the standard system, a lengthy path of legalisation needs to be embarked on: the procedure must be specified, DPOs, councils of different units and the works council have to be consulted before the new procedure can be adopted. It has been recognized, though, that this path of legalisation is an intensive one: it can take up to two years until a procedure is finally defined. In practice, it follows that operations outside the standard systems do and will happen – but this reality can be handled either blindly, or in a reflected fashion. "At least ask your works council", is the simple, but effective attitude voiced about this: do not operate in silence. Communicate your needs and problems.

5.2 Solutions in practice require communication

This need for *un-silence* is particularly strong still in the aftermath of scandal. There seems to be a very high demand for information and a "not yet quite relaxed" atmosphere, especially on the part of the management, which has seen colleagues fired[12].

These challenges are at the heart of conversations about data protection developments: changing the procedure of *deciding about procedures*. Put differently, the hope voiced is to be able to converge rules and practice on an ongoing basis - whenever insecurities arise. This means, of course, that considerable time will be invested in these decision-making processes and that sometimes business processes will be slowed down. The first step is already a big task: the directory of procedures needs to be compared to real practice and adapted so that all activities are well documented.

On the upside from the point of view of the corporation, assuming that rules can be adapted to better grasp the content of actual business activities, a gain in efficiency can be expected over the course of a few years. Most importantly, rules will then be known to all the actors involved; practices will be open instead of covert, and actors will likely be more satisfied with the results of negotiated decision making. Lastly, such documented processes of adaptation provide infrastructures of accountability for everyone to revisit.

Of course, what with such vast changes, there is criticism as well: while the new structures in place are considered adequate by most, the cost question has come up, as well. Clearly, the risks associated with data protection failure are not easy to assess (even though the penalty inflicted on the DB was very concrete), and benefits in trust and atmosphere are even more intangible. Taking into account the conclusions about *measuring the atmosphere*, however, it seems beyond question that the effects of the new data protection structures and communication are tangible, indeed, even if not in quantitative figures.

12 In an earlier interview with a security association representative, we have heard a similar judgement: „The day that Mehdorn had to leave - that's when the managers knew that this topic can turn into their problem. "

6. Conclusion: putting data protection to practice is a process of communication

In this chapter, we have argued that the translation of privacy and data protection law into organisational practice must be understood as a process of communication. Building on our earlier findings about massive gaps between data protection law and practice in the security sector, we have analysed the case of the Deutsche Bahn, which underwent scandal and subsequently reorganised its privacy and data protection infrastructure fundamentally.

The case exemplifies the role of communication as an ongoing process of rule negotiation, implementation of structures, and knowledge transfer in organisations. Data protection law as it is codified is not a plug-and-play device - the legal text needs to be translated with respect to every activity carried out in a company. The DB has recognized this challenge and - in the aftermath of major failure - has moved through an extensive process of negotiating the new formal rules for privacy protection in the company, as well as communicating them to as many employees and managers as possible.

The goal of this process is not to end up with a static set of rules and responsibilities that take care of data protection once and for all, but to rebuild trust within the organisation and find ways to deal with insecurities in the future - openly. The fact that insecurities exist and will always emerge as a function of business activities and technological changes is entirely acknowledged and reflected in new approaches, as the discussion of data processing inside and outside of standard systems has shown. Translation is becoming a regular task, and communication is its method.

References

Alhadeff, Joseph, Brendan Van Alsenoy and Jos Dumortier. "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions." In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. Palgrave Macmillan, 2012 (forthcoming).

Article 29 working Party. "Opinion 3/2010 on the Principle of Accountability", 2010. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf [last accessed 1.3.1012]

Bennett, Colin J. "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats." In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. Palgrave Macmillan, 2012 (forthcoming).

Bennett, Colin J. "International Privacy Standards: Can Accountability Be Adequate?" *Privacy Laws and Business International* 106 (2010).

European Commission. "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union.", 2010. URL: http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf [last accessed

1.3.1012]

Gellert, Rapha・, and Serge Gutwirth. “Beyond Accountability, the Return to Privacy?” In *Managing Privacy through Accountability,* edited by Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. Palgrave Macmillan, 2012 (forthcoming).

Carla Ilten, Guagnin, Daniel, and Leon Hempel. “How Can Privacy Accountability Become Part of Business Process?” *Privacy Laws and Business International*, no. 112 (2011): 28-20.

Guagnin, Daniel, Leon Hempel, and Carla Ilten. “Privacy Practices and the Claim for Accountability.” In *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, edited by René Von Schomberg. Luxembourg: Publication Office of the European Union, 2011

Guagnin, Daniel, Leon Hempel, and Carla Ilten. “Bridging the Gap: We Need to Get Together.” In *Managing Privacy through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo. Palgrave Macmillan, 2012 (forthcoming).

Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, eds. *Managing Privacy Through Accountability*. Palgrave Macmillan, 2012 (forthcoming).