INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L'HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

GERMANY COUNTRY REPORTS

UNIVERSITAT HAMBURG, GERMANY

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN GERMANY – PROFESSOR NILS ZURAWSKI

LOCATING THE DATA CONTROLLER IN GERMANY – PROFESSOR NILS ZURAWSKI

SUBMITTING ACCESS REQUESTS IN GERMANY – PROFESSOR NILS ZURAWSKI

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN GERMANY

Application (primary and secondary legislation) and interpretation (case law) of data protection principles

Primary and secondary legislation

Germany's data protection legislation is fundamentally ruled according to the Bundesdatenschutzgesetz (BDSG, *Federal Data Protection Act*). It applies wherever federal bodies are concerned or where federal law is administered by state level governing bodies in one of the 16 Bundesländer (federal states) within Germany. Each of the 16 Länder does also have a data protection law that is applied to Länder and communal issues. Although there might be differences in details, those laws are overall similar. Occurring differences may have to do with the kind of bodies that may be existent on a federal, but not on a state level. For a general analysis existing differences are not important as they do not touch on the principles of German data protection law.

The BDSG (latest version: 11 June 2010, aktualisierte, nicht amtliche Fassung)[1] is divided into the following sections:

Part I: General and common provisions
Part II: Data processing by public bodies
Part III: Data processing by private bodies and commercial enterprises under public law
Part VI: Transitional provisions

Data protection issues are regulated within these four parts. This includes (among others) issues such as access rights (rights of the data subject), as well as the role of the data protection authorities and data protection officials (DPA and DPO, §4f & §4g), on the federal, state, communal level and in all private bodies. The BDSG has 48 articles and many subsections. All in all around 1000 articles (§) of data protection law exist in various laws (national or federal state level). In addition there are around 100 cases concerning this issue. Thus it is far too complex to be adequately described in detail in this report. However, the section below will try to highlight some of the most important case law which illustrates the ongoing discussion and the application of the principles as laid out in the BDSG. Before doing so, it is necessary and helpful to take a look at the few guiding principles, basic ideas and laws that made this act possible in the first place and which must be considered here, especially regarding subject access rights.

According to all commentaries and leading legal scholars dedicated to constitutional law[2], the guiding principle of German data protection law lies in the 1983 ruling by the German

[1] Federal Data Protection Act (BDSG) in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009. Further changes to the BDSG became effective on 1 April 2010 and 11 June 2010. An up to date and unofficial version of the BDSG can be found here: http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/BDSG/BDSG_node.html (last accessed 20 December 2013).

[2] See for example Killian, Wolfgang, "Germany"; in James B. Rule and Graham Greenleaf (eds) "Global Privacy Protection. The first Generation". 2008, pp.80-106; Papier, Hans-Jürgen, "Verfassungsrechtliche Grundlegung des Datenschutzes"; Jan- HinrikSchmidt and Thilo Weichert, "Datenschutz", Bonn,

Constitutional Court on the then planned census and the formulation of the principle of informational self-determination[3]. This concept refers to the idea that citizens hold the right to be informed about the uses of their data, when collected, used or forwarded by public or private bodies and enterprises; and the right to determine (within the boundaries of the applicable law) what data they give away. This right of informational self-determination is not part of the Grundgesetz (GG, the German Constitution), but is based on leading principles therein. Neither is data protection mentioned in the GG. The BDSG is the current legislation that holds all data protection principles that can be traced back to a few constitutional principles. One of these is Article 10 of the Grundgesetz (GG, the German Constitution) which deals with postal and telecommunication secrecy, i.e. the right not to have one's telephone or email tapped or tampered with. Article 13 deals with the infringement of the private sphere. It consists of seven main provisions, as follows.

"Article 13 - Inviolability of the home
(1)The home is inviolable.
(2) Searches may be authorised only by a judge".

Exceptions to the principle of the inviolability of the home are foreseen in specific circumstances only (Paragraphs 3-7 of Art. 13). Technical means of acoustic surveillance of any home may be employed "if particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law", to "avert acute dangers to public safety, especially dangers to life or to the public" or "for the protection of persons officially deployed in a home", in which case the surveillance measure is ordered by an authority designated by law (Paragraphs 3, 4 and 5, respectively). Interferences and restrictions are permissible to "avert a danger to the public or to the life of an individual" (Paragraph 7). Moreover, Art. 13 states that "the Federal Government shall report to the Bundestag annually as to the employment of technical means pursuant to Paragraphs (3) (4) (5) of this Article. A panel elected by the Bundestag shall exercise parliamentary control on the basis of this report. A comparable parliamentary control shall be afforded by the Länder" (Paragraph 6).

Article 13 provides a strong basis for privacy, the regulation of surveillance and its control. The second important principle that applies to data protection is human dignity (§ 1 of the GG). It was the source of the above mentioned highly important ruling on the 1983 census. The ruling was based on §1.1 GG, which states that "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority. This provision should be read in conjunction with §2.1 about personal self-determination:

> "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law".[4]

Privacy and data protection rights have been interpreted by the German Constitutional Court as the right to informational self-determination and autonomy and it has often followed this

---

Bundeszentrale für politische Bildung 2012

[3] Bundesverfassungsgericht (German Constitutional Court) decisions volume 65, p. 1 ff.

[4] Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 21 July 2010 (Federal Law Gazette I p. 944). Translation taken from: http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0015 (last accessed 20 December 2013).

principle in further cases, such as the planned act for enhanced acoustic surveillance of private spaces, which was ruled against with reference to Art. 1 GG.[5] This explains why the bases for data protection under German law can always be traced back to Art. 1 of the GG. According to the constitutional court informational self-determination is vital and a part of human dignity. Although the term "informational self-determination" cannot be found in the GG (basic law) and only appears in the 1983 ruling, it has become the guiding principle of all data protection law that followed in Germany (see for example the case further below).

The constitutional court made this ruling in response to the census law of 1983 that was challenged and subsequently declared unconstitutional (BVerfGE 65,1 - Census Case).[6] In light of the approaching year 1984, the epistomised date of the surveillance state, in conjunction with a vibrant culture of social unrest and protest that had come out of the 1960 student protest and had started to spread into many realms of life in Germany, the planned census became a focus point for resistance in the early 1980s. The surveillance state and the privatisation, informatisation, and centralisation of data (thus the infringements on the private sphere), became part of the driving narratives of the movement against the central census planned for 1983. Hannah suggests that this movement was the earliest mass movement addressing issues of the information age[7]. The image of Big Brother loomed all over the discussion and hence made the impact of the protest quite severe. Additionally the 1970s saw a wave of terrorism in Germany and the State reacted with new measurements, such as dragnet investigation, early forms of police profiling, suspicion, bans on people being employed in public service (especially teachers), because of politically (mainly left) affiliations[8] and so forth. It was these experiences that added to the unease and consequential protest. One way of protesting this census was its challenge at the Constitutional Court. Ultimately, the court's ruling led to the census being postponed, and the Constitutional Court issued a ruling that made it necessary to rewrite the census and indeed gave birth to a new understanding of data protection.[9] It must be stressed that these developments were the culmination of longer unease with new information technologies, stored data and the fear of a surveillance state, which may be a legacy of German history, especially between 1933 and 1945. From 1970 onwards, the first data protection laws were passed in state parliaments and also the federal parliament (Bundestag) as a reaction to these debates. The 1983 protest set this debate on the national agenda and made it widely known in the public sphere. After 1990, when West and East Germany reunited data protection was a major aspect of public politics did not cease, also due to the experiences with an oppressive, authoritarian (socialist) regime that had established an almost perfect surveillance state in East-Germany[10] and left a traumatic legacy on the life of many people as well as in the German collective memory[11].

As a result of decades of public politics, independent rallying by pressure groups and a raft of legislation, Germany today has 17 laws on data protection, i.e. one for the federal state and

---

[5] German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. (1 - 373) judgment of 3 March 2004 - 1BvR 2378/98 and 1BvR 1084/99, available at: http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html (last accessed 20 December 2013).

[6] Killian, 2008 op. cit. and Papier, 2012 op. cit. For details on the census case, see Hannah, Matthew, "Dark Territories in the Information Age. Learning from the West German Census Controversies of the 1980s", Farnham, Ashgate, 2010

[7] Hannah, 2010 op. cit

[8] See for example the order on radicals, *Radikalenerlass.*

[9] Killian, 2008 op. cit.; Hannah, 2010 op. cit. and Papier, 2012 op. cit.

[10] Gieseke, Jens: Die Stasi, München, Pantheon, 2011

[11] von Lewinski, Zur Geschichte von Privatsphäre und Datenschutz - eine rechtshistorische Perspektive. Jan-Hinrik Schmidt and Thilo Weichert, "Datenschutz", Bonn, Bundeszentrale für politische Bildung 2012

one for each state (16) of the republic that hold the provisions for state level, local and communal administrations. These do not differ to a great extent and are all based on the same principles. There may be minor differences and interpretations, but the principles of data protection law are consistent between those 17 pieces of legislation. Other legislations that have an impact on issues of data protection in Germany deal with specific technologies and its subsequent techno-social assemblages, i.e. telecommunication and the internet. Data protection issues regarding forms of electronic communications are either dealt with in the *Telekommunikationsgesetz*, which addresses the telecommunications sector (telephone, mobile communications), or in the *Telemediengesetz*, addressing data protection issues in so called telemedia, such as Internet, TV, etc. Both are federal laws.[12]

Most recently in January 2014, the German Federal Court of Justice delivered a judgement clarifying how data controllers should respond to subject access requests concerning credit scoring. Specifically, the judgement ruled on the scope and extent of disclosures and whether data controllers had to provide an explanation of how the scoring algorithms used in their credit rating practices calculated certain factors as well as disclosing what reference groups used to calculate a credit score are made up of[13].

The court decided that data controllers did not need to disclose the above information in responding to access requests. While personal data should still be disclosed, in line with Germany's data protection legislation, the court found that trade secrets such as credit scoring algorithms should still be protected. As a result, something of a compromise was reached between Germany's long-established legislative commitment to transparency in data protection matters and protecting the secrecy of credit scoring agencies' working practices.

Interpretation (case law)

The principles mentioned above inspire data protection and find their way in national courts. This emerges from recent case law which illustrates how German courts have ruled on new technology developments on the basis of the BDSG and its leading constitutional principles.

Online warrants and online search of computers – this ruling was made by the constitutional court, 1 BvR 370/07 of 27.2.2008.[14] The subject-matter of the constitutional complaints were the provisions of the North Rhine-Westphalia Constitution Protection Act regulating, firstly, the powers of the constitution protection authority regarding various instances of data collection, in particular from information technology systems, and secondly, the handling of the data collected. The ruling of the federal court dismissed the case, but based its decision on the following principles:

1. The general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (Grundgesetz – GG)) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems.

[12] For an oversight of all existing legislation in Germany, see: http://www.datenschutz.de/recht/gesetze/ (last accessed 20 December 2013).

[13] Press release of the judgement available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2ef8cefa03b7d0493f54c1bc71ee0a53&anz=1&pos=0&nr=66583&linked=pm&Blank=1 (last accessed 14 April 2014)

[14] German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), judgment of 27 February 2008, available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html (last accessed 20 December 2013).

2. The secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest. Predominantly important are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence. The measure can already be justified even if it cannot yet be ascertained with sufficient probability that the danger will arise in the near future insofar as certain facts indicate a danger posed to the predominantly important legal interest by specific individuals in the individual case.
3. The secret infiltration of an information technology system is in principle to be placed under the reservation of a judicial order. The statute granting powers to perform such an encroachment must contain precautions in order to protect the core area of private life.
4. Insofar as empowerment is restricted to a state measure by means of which the contents and circumstances of ongoing telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against Article 10.1 of the Basic Law alone.
5. If the state obtains knowledge of the contents of Internet communication by the channel technically provided therefore, this shall only constitute an encroachment on Article 10.1 of the Basic Law if the state agency is not authorised to obtain such knowledge by those involved in the communication.
6. If the state obtains knowledge of communication contents which are publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle it does not encroach on fundamental rights.

Although the case was dismissed, it shows that the GG and especially its basic articles which are the guiding principles for the Data Protection Act, play a very important role in the arguments.

Another example is the constitutional complaint challenging §§ 111 to 113 of the Telecommunications Act (Telekommunikationsgesetz – TKG).[15] Although the challenge was unsuccessful, the court ruling stated that parts of the act were in violation of the right to self-determination. Here the court recognised that the "First Senate of the Federal Constitutional Court held that the collection and storage of telecommunications data under § 111 TKG and their use in the automated information procedure governed by § 112 TKG are constitutional". However, "§ 113.1 sentence 2 TKG is not compatible with the right to informational self-determination. But the provision is to continue in effect on an interim basis, until 30 June 2013 at the latest, provided that the access codes may be collected only subject to the conditions which, under the applicable provisions in each case (for example the provisions of criminal law), govern their use".

Both cases show that the original concept of the right to self-determination continues to play a vital role in court arguments in individual cases. However these cases and many others more do not necessarily impact on the existing BDSG, but interpret the BDSG or its ruling principles as set out in the GG, especially § 1,1 and 10 (see above) in its favour. As these examples show, although data protection is highly threatened by surveillance practices nowadays, the GG represents a robust safeguard to counter illegitimate surveillance practices. Similarly, the BDSG supports claims by citizens and gives them a strong tool to challenge

[15] German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 1299/05, order of 24 January 2012, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg12-013en.html (last accessed 20 December 2013).

infringements and modify acts and new laws that may infringe and impact on privacy rights and informational self-determination.

Application (primary and secondary legislation) and interpretation (case law) of the right of access to data

Specific provisions that concern access rights can be found in the BDSG and in particular at Articles § 19 (public) and § 34 (non-public), "Auskunft an den Betroffenen" (*advice to the parties involved*).

Article 19 enlists the rights of data subjects (in the public sector). It holds that, upon request, data subjects shall be given information on:

1. recorded data relating to them, including information relating to the source of the data,
2. the recipients or categories of recipients to which the data are transferred, and
3. the purpose of recording the data.[16]

The same provision applies for access rights in the private sector (Article 34). It may also be interesting to note that § 33 of the data protection law states that one must be notified when data is taken the first time. In fact, if "personal data are recorded for own purposes for the first time without the data subject's knowledge, the data subject shall be notified of such recording, the type of data, the purpose of collection, processing or use and the identity of the controller".[17]

An important part of Articles 19 and 34 is the notion that data must be related to the person (original: *die zu seiner Person*). In effect, this could mean that images (such as those captured by CCTV) without any trace to personal data, such as name or address may not fall under this law and such data may therefore not be disclosed following a subject access request. While Hoss[18] states that the right to access is an inalienable right (§ 6 Abs. 1 BDSG) and any infringement or restriction is unlawful, he also states that many non-public sector actors do not comply with this law and do not give subjects access to their data - despite it being a misdemeanour, subject to fines and payments. Roßnagel states that this particular right has the status of a magna carta of data protection, as this is the important right through which citizens are enabled to decide whether or not data shall be used in the way it is used[19].

In general, subject access rights are regulated on the basis of both articles. In both public (§ 19) and private cases (§ 34), the information should be given out without a fee. Information

[16] Federal Data Protection Act (BDSG), in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009, available at: http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile (last accessed 20 December 2013).

[17] Ibid. For all relevant case law concerning the legislation under 1 and 2, see Kilian, 2008 op. cit. and Papier, 2012 op. cit.

[18] Hoss, Dennis, "Auskunftsrecht des Betroffenen aus § 34 Abs. 1 BDSG in der Praxis: wirksames Instrument oder zahnloser Tiger", Juris, RDV 2011, 6-11. See also Mallmann, Otto, "Zum datenschutzrechtlichen Auskunftsanspruch des Betroffenen", GEWERBE ARCHIV (GA): Zeitschrift für Gewerbe- und Wirtschaftsverwaltungsrecht Nr. 9 vom 09. September 2000, p. 354.

[19] Roßnagel, Alexander, Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München, Beck, 2003

held by public institutions may include underlying restrictions when it comes to secret services or other data that may interfere with state affairs. In those cases, DPAs may serve as an intermediary and be given the data which then might be transferred to the data subject. Private data may underlie restrictions in terms of their commercial value and there may be a requirement to pay a fee, when the data may be used for commercial purposes. Neither § 19 nor § 34 say anything about the duration of answers to such requests. No particular point of contact is identified for such requests in the legal text, which reads as if one may address the request to the company or public body in general. Art. 19 establishes specific circumstances in which data shall not be withhold, namely in case:

1. the information would endanger the orderly performance of tasks for which the controller is responsible,
2. the information would threaten the public security or order or otherwise be detrimental to the Federation or a Land, or
3. the data or the fact of their recording, in particular due to the overriding legitimate interests of a third party, must be kept secret by law or due to the nature of the data, and therefore the data subject's interest in obtaining information shall not take precedence.

In case the data subject has been denied access to personal data, he might challenge this decision by addressing to the Federal Commissioner for Data Protection and Freedom of Information, under specific circumstances. Art. 19 establishes that "no reasons must be given for refusing to provide information if stating the actual and legal grounds for refusal would threaten the purpose of refusing to provide information". However, in this case, "data subjects shall be informed of the possibility to contact the Federal Commissioner for Data Protection and Freedom of Information". Moreover, "if no information is provided to the data subject, at the data subject's request this information shall be supplied to the Federal Commissioner for Data Protection and Freedom of Information unless the relevant supreme federal authority finds in the individual case that doing so would endanger the security of the Federation or a Land. The information provided by the Federal Commissioner to the data subject may not provide any indication of the knowledge available to the controller without its consent".

A prominent case in Germany concerning subject access requests is that of Malte Spitz, a member of the Bundestag (the federal parliament). Spitz sought to have access to his mobile phone data but was denied access to this data by the German Telekom. As a result, he sued the company in order to access the data and was successful in doing so. He eventually received his data for a six month time period between August 2009 and February 2010. Spitz's case also related to the debate around the length of retention of certain types of data. The Data Retention Act, which was passed in Germany in November 2007, allowed for a six month storage time for telecommunication data. Since its enactment into Germany law, the Act has been challenged and in March 2010 the German Constitutional Court ruled that the Data Retention Act does not comply with Art. 10 of the GG *"Privacy of correspondence, posts and telecommunications*".[20] Spitz and the Germany weekly "Die Zeit" used the data

[20] Federal Constitutional Court, (Bundesverfassungsgericht), 1BvR 256/08 of 2.3.2010, paragraph no. (1 - 345), judgement of 2 March 2010, available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (last accessed 20 December 2013). For the English press release on the ruling, see: Federal Constitutional Court, (Bundesverfassungsgericht), http://www.bverfg.de/pressemitteilungen/bvg10-011en.html (last accessed 20 December 2013).

obtained from German Telekom to prove how such data may be used to track people and generate profiles of location and media use.[21]

National exceptions to the EU Data Protection Directive and to the right of access to data

The BDSG does not provide for exceptions that fall out of the scope of Directive 95/46/EC and instead, it recalls the provisions of the Directive. Art. 10 of the Directive imposes on data controllers the obligation to notify data subjects about the purposes of the processing for which the data are intended (indent (b)). This obligation is also established by the BDSG at Art. 4. However, it is important to note here that the BDSG does not provide any obligation to notify the data subject about the logical construction of a possible automated processing which concerns the data subject[22].

Compatibility of national legislation with Directive 95/46/EC

The EU Directive was implemented in 2001 in German legislation. Since then, the compatibility of national legislation with European data protection norms has been questioned on several occasions. In 2005 the European Union reprimanded Germany for a non-sufficient implementation as the Länder-data protection officers were deemed not to be independent enough. The European Commission initiated infringement proceedings against Germany in 2001 and 2005. In 2010 the European Court of Justice (ECJ) pronounced itself on the independence of German data protection authorities and condemned Germany formally and plainly.[23] In the case European *Commission v. Germany* of 9 March 2010 the court argued that German regional DPAs were considered to be insufficiently independent, since they were part of the regional administration and subject to State scrutiny. The lack of independence of German DPAs was against Directive 95/46/EC and constituted an infringement of its provisions.

Surveillance and access rights: codes of practice at national level (CCTV and credit rating)

As laid out in the BDSG § 34, various articles in the BDSG regulate the liability to notify the person that data will be collected and stored. Different regulations exist for public and non-public actors. § 33 (liability of notice) regulates the notification for the non-public sector, while an explicit regulation is still missing for the public sector. In these cases the notification is regulated within § 4(2) BDSG in conjunction with § 13. Public actors must obtain data directly from the subject, so that he/she may perform his/her right of informational self-determination. § 4 outlines that the subject has to be notified as to the reason for the data collection in each particular case. In addition §16 regulates the notification of subjects, if their data is passed on to non-public actors. CCTV images collected of a person may not be accessed if no other data related to the person is stored. The image itself, without any other data relating *to* the person is not subject to such requests and may not be given out. According to information provided by the DPA,[24] this also serves as a security measure to

[21] Biermann, 2011, http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz also: http://malte-spitz.de/2011/03/04/six-months-of-my-life-in-35000-records/ (last accessed 20 December 2013). The same story in his own account can be found on his website in English.
[22] Roßnagel, 2003, op. cit.
[23] ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010.
[24] Personal information provided via telephone.

prohibit third parties that may know a person on such images to request such images and hence have personal details (who, when, where) without permission of the person in question. As for credit rating, the "SCHUFA", a common enterprise of banks and other credit giving businesses is widely known in Germany. For many commercial transactions, one has to sign a lease so the credit giver (landlord, banks, mobile phone companies, car dealers if paying in rates) may obtain a credit rating about the person. Each person in turn has the right to get their own data and the credit score for free. There are other services for customers and commerce alike that cost money, but in general the SCHUFA is well known and almost every citizen had at least heard of it, as it is a vital part of credit businesses in Germany.

The promotion of access rights by DPAs and national authorities and their role in ensuring compliance to national norms

Most of what the German DPAs do remains unknown to the wider public. Although the annual (or biannual) reports are full of activities, this is not widely known. However the DPAs as institutions are more or less widely known as data protection bodies, especially since such contested cases like Google Street View, Facebook's privacy policies or the latest NSA scandals are discussed at length in the media. This is usually the medium where various DPA officials (federal and state level) serve as experts and present strong opinions or even challenge companies or state institutions with legal actions. Whether they also promote access rights in particular and to what extent cannot be extracted from their reports. DPAs promote the use of rights and raise awareness for data protection issues on various levels, e.g.: on their websites, where they provide the legislative texts, brochures on various topics, e.g.: Facebook, loyalty cards, workplace surveillance, freedom of information and many more. The federal as well as all state DPAs' websites provide a wide array of resources to get informed about data protection. However given the size of their administrations, it seems impossible to extend their reach by other means. The federal DPA has 85 people in its office, Hamburg's DPA has 20 persons working in different areas. This is far too small, particularly in light of the latest report which approximates that they have to oversee around 160,000 enterprises in Hamburg alone. The DPA of the city of Hamburg reports that 1,700 written complaints were received in 2010 (last available report covering 2010 and 2011). The federal DPA meanwhile, reports of 9,729 received complaints in 2011/2012. Neither report however, states the nature of these complaints.

The role and tasks of DPA and DPO, which seem to conflate are ruled in Article § 4f and g of the BDSG. According to Article § 4f, both public and private bodies which process personal data shall appoint a data protection officer. Private bodies shall do so within one month of commencing their activities. This obligation does not apply to private bodies in which no more than nine persons are permanently employed. However, a data protection official should always be appointed "where private bodies carry out automated processing subject to prior checking, or commercially carry out automated processing of personal data for the purpose of transfer, transfer in anonymous form or for purposes of market or opinion research". Data protection officers should have certain personal and professional skills to perform their duties, such as competence, reliability, secrecy and independence. Their professional profile is characterised by a high level of specialised knowledge in dealing with personal data. Art. § 4 f of the BDSG establishes that data controllers should make sure that their DPOs keep that level of competence enabling them to take part in advanced training measures. The expense of such measures shall be assumed by the data controllers themselves. Accordingly, this makes data controllers responsible for the protection of personal data and for their own data protection policies and practices. In fact, data controllers shall "support data protection

officials in performing their duties and shall provide assistants, premises, furnishings, equipment and other resources as needed to perform these duties". The BDSG recalls that data subject should be free to contact DPOs at any time. In turn, DPOs may consult the German DPA (Art. 4g).

Art. 4g enumerates the main tasks and responsibilities of DPOs. In particular, they shall:

1. monitor the proper use of data processing programs used to process personal data. For this purpose, the data protection official shall be informed in good time of projects for the automated processing of personal data;
2. take appropriate measures to familiarise persons employed in the processing of personal data with the provisions of the BDSG and other data protection provisions, and with the various special requirements of data protection.

Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights

DPAs serve as the first point of contact if citizens have problems with data protection or want to report, know or educate themselves. Germany's data protection laws give the DPA a substantial role with regards to access rights, especially in cases where public institutions do not want to provide data directly to the data subject. DPAs may act on behalf of citizens, but also have the duty to control legislation, products, and procedures of public and non-public entities, i.e. administrations, public bodies or private companies - both for profit and non-profit purposes. The role of DPAs is laid out in the BDSG, § 4f and § 4g.[25]

As explained above, alongside the work of DPAs, all companies and public bodies are legally bound to appoint a Data Protection Officer (DPO) depending on the size of the organisation or the amount of data collected and processed as part of its activities. Such a DPO may either be an employee or an external consultant that has sufficient knowledge in the field of data protection. The federal and the state level DPAs are the supervising bodies to those ground level DPOs in companies or public authorities. Whether special measures are taken to promote subject access requests and to spread the knowledge about this right could not be found explicitly. Generally speaking however, it seems that access rights are not a priority in the activities of German DPAs. Searching the large database of the federal DPA however, does yield many results that are concerned with various fields for access requests, including how to make a request to Europol or to the Bundeszentralregister (Central Bureau of Justice, a federal agency) for obtaining information on police records, if not done through your local administration. DPAs at federal as well as state level may also provide assistance and in some cases may serve as intermediaries to access those rights by law (see above). All other duties are related to the provisions cited in the previous section (6).

[25] A description of the work the German DPAs can be found in the Deliverable 3 of the EU FP7 project PRESCIENT (Privacy, data protection and ethical issues in new and emerging technologies), "Assessing citizens' concerns and knowledge of stored personal data", 15 May 2012, available at http://www.prescient-project.eu/prescient/index.php (last accessed 20 December 2013).

LOCATING THE DATA CONTROLLER IN GERMANY

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details of 32 Germany-based sites. In particular, the examples below are illustrative of the individual researcher's experiences conducted in Hamburg and do not claim to reflect the practices of *all* data controllers in Germany. This report illustrates some general trends noted alongside examples of good and bad practices encountered during the course of this research.

Overall impressions

Locating data controllers in the German context was reasonably straight forward in most cases. ourWe were able to locate almost all data controllers or their addresses via the web, by telephone or in person. Of the 32 sites we visited, we successfully located data controllers in 26 cases. However, in all cases we were able to find a 'lead' for further investigation which means that in every case, we were able to find *some* information about the data controller if not locate the data controller itself. Of the 26 data controllers that were identified, we were able to locate 14 data controllers by finding a named responsible individual. Of these, 11 were located online.

Data controller contact details successfully identified	26 out of 32
Data controllers unable to identify	5 out of 32
Data controller identified via online privacy policy	21 out of 32
Data controller identified via the telephone	3 out of 32
Data controller identified in person	2 out of 32
Average rating given to visibility of privacy content online	2 - Adequate
Average rating given to quality of information given by online content	2 - Adequate
Average rating given to visibility and content of CCTV signage	1 - Poor
Average rating given to quality of information given by staff on the telephone	2 - Adequate
Average rating given to quality of information given by staff in person	1 – Poor

We experienced differences in the responses of members of staff when asking in person or searching over the web compared to speaking on the phone. It seemed that the information given by phone was often better in those cases where questions arose and information was

unclear on the web. Such questions could not be answered when being on the web. However, it has to be said that looking on websites was usually the easiest way to locate data controllers. Overall it can be said that finding information on data controllers was relatively straightforward and this may be attributable to Germany's federal data protection laws (BDSG, and its local variations in the states). These regulations give quite consistent and binding guidance as to how public and private bodies have to respond to citizen queries and how they must be prepared to be visible and informative on matters of data protection and privacy.

When searching via the web, one has to be aware that it is easy to find information on data protection issues - mostly located at the bottom of each site - however, such information usually concerns the data issue connected to the use of the site only, i.e. cookies, storing your IP address and so forth. This rarely gives you any further detailed information or hints where to find this site's data controller or any information about subject access.

When searching for data controllers via the web it has proven to be very good to either use the search functions provided at the site - and most sites do provide this function; or to actually use Google to look for the pages, where such information is provided. This strategy in particular leads to a methodological question discussed further below.

Methodological remarks

Most of the sites posed no problems, mostly so, because they were national or international commercial sites. To locate a data controller varied along these lines. It was more difficult to find a multinational data controller for instance, than it was for a national supermarket or other more nationally relevant organisations.

We would like to share some methodological thoughts on the issue of using search functions or search engines (such as Google) to locate data controllers. We are aware that using a search function to find the data controllers is being based on the knowledge of the particular search strings and the knowledge of the existence of such a right and the right terminology. The methodological design of this research was based upon the researcher acting as a so-called lay person and therefore lacking awareness around the issues of data protection and privacy. However, during the course of this research, as much as we were trying to look through the eyes of someone that has not done this before or does not have our knowledge, we must say that whoever is aware of his or her right to access his or her personal data and its uses, is well aware where to look for or whom to ask. And if not on a particular site, then he or she will approach the local DPA - 16 DPAs in the 16 federal states of Germany - and ask for help. And these indeed provide excellent help through their websites or even on the telephone. Data protection in general is an issue that actually many people know about in Germany. It is widely and often discussed in the media, the DPAs are very visible and known to many people. Not necessarily by name, but by institution. Once interested in the subject as such, the DPA is easy to find via a Google search, probably the instrument of choice in locating something on the web in the first place. From previous research on loyalty cards[26] we know that although the issue of data protection did not play a role in reason to accept or deny a loyalty card or the membership to such a programme, most of the then interviewees of

[26] Zurawski, Nils: Local practice and global data. Loyalty cards, social practices and consumer surveillance– Sociological Quarterly, Volume 52, Issue 4 (winter) 2011
Zurawski, Nils. Consuming Surveillance: Mediating Control Practices Through Consumer Culture and Everyday Life, in: Jansson, André / Christensen, Miyase (eds.) Media, Surveillance and Identity, New York u.a. 2014, Peter Lang.

the study knew about the issue in a way that suggests to us that they would know where to go to in the case of a problem or request. This leads us to think that the right to subject access requests has the precondition of rather special knowledge.

As such, if someone wants to make a subject access request, knowing the search strings to locate relevant information as part of that process is part of this knowledge. The other option would be to contact one's local DPA and ask for advice. To assume that a lay person may be able to make a subject access request, means to assume this knowledge. The one does not come without the other. Hence, search engines are a viable option to find the contact addresses, even if a clear link on each page to make such requests would be a great improvement of the law and put it into action. Without it, it remains a law for people with a special knowledge. There are no lay persons performing this task - you either know, or you do not. In the last case, you do not come up with the idea to make such a request. While we cannot claim to have one true explanation as to why DPAs are so prominent in Germany, we can think of a few reasons. The issue of data protection has a large and continuing legacy in Germany, reaching back to the census boycott of 1983 and the subsequent legislation of "informational self-determination" based on the dignity of the person. Ever since, issues concerned with data protection in one way or the other have always attracted media attention, including DPA' official's appearances on prime time TV on various issue - from loyalty cards to the NSA scandal, from data fraud to the latest census. However from our own research we can say that data protection must be seen as somewhat "contextual or situational" knowledge. That means that it is not present in many of the routine activities and aspects of everyday life, but a strong subject in its own right, only being recognised when being directly addressed. According to the question of the lay person, this would mean that many people are in fact "sleeping" experts, but as data protection does not play a role as mundane activity of everyday life, knowledge only comes to the fore when faced with a problem - when in turn the person ceases to be a layperson in the true sense. Some people are more knowledgeable than others, which means that general information about the rights and the possibilities to act upon them should be made more visible and indeed better known as such. Putting data protection on the front of companies' homepages however will not help, as long as you are not interested in the issue as such. The rights connected to data protection should rather be taught in school, similar to the right to vote or other basic human rights. The chance of them ceasing to be "addressable" knowledge surfacing only contextually seems to be much higher that way. There must be a data protection education, that would include the rights to access one's own data and many more aspects.

Public sector

The institutions of the public sector seem to follow the required practice of displaying the data controller rather well. However, in some cases it was unclear whether to categorize an institution as being in either the public or private sector - for example the health sector. For this report we have subsumed them under public, although this is not entirely correct - but notwithstanding the structure of the health system, it is widely state monitored and follows a structure that is under public control. As for data control, there is no national health record, nor does a central record exist on a local basis. Medical data is stored with the doctor one goes to. So all medical data is dispersed depending on how many doctors we ask for advice. Some of this data is stored with the health insurance of our choice (or hospitals if attended). As the German system differentiates into a so-called public insurance (with many private companies offering this obligatory service) and private ones (voluntary if one is over a certain annual income), the data is held by the insurance a person is insured by. The insurance does not hold the same data as the given doctors do, but in the case of the public ones, they are

given the according ICD[27] code and a rough diagnosis; in the case of the private ones they are given a code according to the tariffs. So the medical data is available only in coded form. The original data sets are all held by the doctors themselves. Doctors have the right to medical confidentiality, which would be breached if the health insurance would actually hold this data other than in codified form or the doctor would sell or otherwise reveal the data to third parties The complete data only exists in a very de-centalised form and in centrally in a codified form at the insurance. No central data is available. The data controller of doctors are the doctors themselves, or if they work as hospital employees, the hospital. As Germany has the right of the free choice of doctors, in theory one could visit a different doctor everyday and have the individual data stored with different doctors, i.e. the data whichconcerns that particular visit. In the case of this research, information about the doctor's data controller was simply obtained by contacting the doctor asking about our data, together with contacting our our insurance by telephone and asking for their data protection officer (DPO)[28].

School records are very much alike[29]. The complete school record of a pupil is held in a file at the school(s) (elementary and secondary) one has attended. The school file travels with eventual school changes. These files usually exist as paper files, not as digital data. Most of those files have to be stored for ten years. After that they are destroyed and only the final exams are stored for further archiving purposes. Some data on pupils does exist at the local level, i.e. at the communal and federal state level for administrative and more general statistical purposes. The data controllers for these data sit within the public administrations of the schools within the school districts. Some of the data is personalised, some is not. The statistical data is de-personalised for instance and mainly used for future planning and performance monitoring of the entire school system within the reach of a school authority. From those two examples it can be said that de-centralised data seems to be a viable form of data protection, combined with general codes of practice of how to handle these data. This information was relatively easy to obtain, as weollowed the way of the data itself, i.e. from the school, to the school overseeing body in the city of Hamburg - both a community and a federal state - and got hold of the DPO within the statistical unit of the school administration. The information provided was adequate and there was absolutely no opposition or scepticism. given the structure of the data storage, it thus seems rather complicated, if not impossible to get hold of a complete health record or school record of a given person. The structure stems from the federal and de-centralised system of Germany's state structure.

This however is different when it comes to criminal records. These are also nationally held, but every citizen can access them by going to the local administration and making a request, paying a fee and getting his or her criminal record (*Führungszeugnis*, clearance certificate). This is centrally stored by the Bundesjustizamt, who have a dedicated data protection officer (DPO) that may be approached. However, in our perception our criminal record is no secret and more or less easy to access by ourself for various purposes, e.g. job application at public employers, obtaining licences for aviation or for particular jobs. The system seems quite transparent, although we cannot check what is actually in the database and what we are being told. But giving credit to the system, criminal records are deleted if barred and should not be

[27]ICD Code: International Statistical Classification of Diseases and Related Health Problems - issued by the WHO

[28] As outlined in Germany's legal analysis above, it is a legal requirement for many organisations Germany to appoint a dedicated Data Protection Officer.

[29] The information about the school records is based on research on the backgrounds of what data is stored where, conducted via phone with the school adminstration. To obtain your school record you would normally go to your (former) school and request to see your file.

in the data base anymore after a certain time (depending on legal standards set in the criminal law).

Related to the justice system is Europol. In their case, we could not find the details of the data controller despite reviewing their website content. However, we could retrieve a 40 page long document on Data protection at Europol"[30]. Whilst this document does not say anything about accessing personal data as a right through the EU directive, it gave good information on which an interested party could rely on and use as a basis to practice that right.

Passports and ID cards are issued through local registry offices (*Meldebehörde)*. The data that is stored with that registry office is the basis of your passport/ID card. Registration with the local registry office is mandatory for every German citizen, as is the obligation to hold a valid ID card. This is ruled in the passport law (Passgesetz (PaßG)) which also outlines that some of the data concerning passports may be transferred for border control purposes. All aspects of the legislation concerning data protection can be found within § 16 of the PaßG. So there again is no central database for the data that goes into a passport/ID card. Due to the federal system, databases are only run and administered locally and have no or only weak ties to other administrations. This also accounts for other local administrations. Data may not be shared by default but by rule of exception. Interestingly, the data kept at the registry office, should be accessible to police and other official sites, which means it should be accurate and up to date. A recent census (2011, published in 2013[31]) however has brought to light that this is not the case and many cities had different numbers of inhabitants than their own records showed. If one moves from one federal state to another, the data is not transferred automatically, but entries are deleted (old place) and renewed (new place) by the citizens themselves. Given the obvious potential for inaccuracy this tells something about the quality of the data being collected and processed. In order to access the data that is being held about a given citizen at the registry office, one must fill out a request form, pay a fee and get all the data available. Interestingly, this can also be done by a third person, i.e. someone else may find out about another citizen's address and name at a local registry office, if they pay the required fee. Citizens have the right to prohibit this information from being given out, but have to opt out for that. The so called Melderegisterauskunft is part of the Meldegesetz (local registry law), which makes mandatory for citizens to register with their local community if they live there. This registry slip is needed for landlords, to obtain a passport, to perform your right to vote, so almost all citizens know about it as part of their everyday life as citizens living in Germany. To find the details on the it is sufficient to perform a google search using the string „meldegesetz hamburg bezirksamt" together or in combination of either of the three (registry law hamburg local adminstration) and find many entries including a Wikipedia entry on the registry law itself.

In general, it can be said that many public services that involve some data management are accessed via the registry office; hence data requests are also issued through this administrative body. The federal system does not allow for a national storage of this data. However there are a few exceptions: a) the police may access all databases and request to know whether someone is registered with a particular address or not. Giving a wrong address will then result in a failing request, but not necessarily revealing the correct address or name. However, car owners' data is held in a national database, which means that police may find a person through a car registration that would reveal the owners address at the given local registry office. As registering at a local level is mandatory, German citizens always leave a

[30] https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf
[31] Census results: https://www.zensus2011.de

trace of data. It is possible to avoid registration, but as many services require you to show your ID or an entry in the local registry, there are little benefits and many obstacles in circumventing this duty. Due to the federal structure of the German state, the codes of practice and the strong data protection laws, we may speak of good practice concerning data protection in many areas of the public sector. However, due to the mandatory nature of the registration, one could also argue that such registration policy is negative in the first place.

Private Sector

In general, data controllers of private companies were relatively easy to find and often quite straight forward. Only few had templates for special requests, but email contacts for general communication and questions could be used to sidestep this, but this is not the same. How a subject access request would be answered in practice cannot really be said from the information given on most websites. All private sector websites that we researched provided at least the address of the company and in some cases contact details for the DPO itself, sometimes with a specific name. If not named, contact details sometimes included a dedicated email address (such as dpo@company.de) or a postal address.

Two examples have to stand out however. To access one's credit scoring data is fairly simple in Germany and an act that is widely known to the public. The *SCHUFA* (a scoring agency owned by banks and other commercial enterprises) is well known as you have to allow a bank to inquire about your scoring details before opening a bank account (which almost all Germans have), for mobile phone contracts, buying a car, house, furniture or else on credit. To get your scoring data from them is their business, so there is no problem finding any information, nor is this considered special knowledge. To find out about their data protection policy one must simply follow the link "Datenschutz" and all aspects concerning the handling of data is explained, including a nameless address for contact to their DPO. As this is the main scoring agency in Germany you do not need to be an expert to find either the website or the information about data protection. To access your actual scoring data is slightly more complicated, as you have to register, prove your identity - as a security measure for fraud and false requests - and then you can access the highly sensitive data on your credit scorings, mortgages, credit details and else.

A second good and very transparent example was that of our employer - in this case categorised as private. As our first point of access to all questions regarding our employment is the HR office in the university's administration, we called the administrative person to ask for our files. Surprisingly we were invited to come any time and take a look at our files and the data stored about us by the university in the HR offices. However, the university does have a data controller, who is part of the upper level of the administration and was also rather easy to locate through the web. We regard this as common practice and a rather good example of information policy.

CCTV and signage

CCTV is a special issue in terms of the data stored. We approached all sites using CCTV in person and some via the website in addition to double check if some information were also available there. Information was quite easy to find, signage was displayed, however never with a phone number to contact. Approaching personnel on site was no problem and the information was usually of good quality. In the case of the local transit authority and the supermarket we were told that the video footage will be overwritten after 24 hours (which in the case of the transport setting we knew before) and only accessed in the case of an incident. So to make a subject access request in these cases would, in theory, be almost impossible

given the very quick data erasure deadlines. These deletion times are subject to regulations wherein CCTV images have to be deleted within 72 hours unless further special needs are claimed by the CCTV operators. The 24 hours deletion was a deal the DPO negotiated with the local transport authority when cameras in trains and busses were introduced in 2003. This follows the principle of data avoidance as no data is good data in this case, and it may also reduce the risk of misuse and aims for a relatively simple technical solution. The larger an institution or corporation, the more likely is that they adhere to this policy. Smaller businesses are less controlled and not so much in the focus of the DPOs. The bank provideduswith a lead to where to go - its headquarters, which in this case is in Hamburg, as it is a smaller union bank in the city[32]. At the post office, we encountered CCTV by accident and had a rather strange experience, as we were told that only the previous 1 hour is recorded in the case of an alarm. As you cannot record the past retrospectively, we inquired further and were met with a slight animosity to our inquiry. We were advised that the data was stored at the national headquarters in Bonn and not locally - unless in the case of an alarm. The advice we were given became even more unclear and inconsistent after that so we left the scene. This case showed that the knowledge of the member of staff regarding data protection issues and the effort make to ensure that we were given the correct information were not of good quality. The willingness to answer further questions was getting smaller with more inquiries and we could see the unease of the member of staff.

In order to seek clarification on this issue, we filed a subject access request on the 23rd of July to the DPO of the company and had a response on the 5th, respectively the 6th in the mail. We received two letters, as we had addressed the initial request to the wrong address. We were misled, as we thought the post offices were run by one company, when in fact they are run by another. They offer postal services of the first company (an express delivery service) as in-house services. The first letter informed us about this misunderstanding, but also informed us about forwarding our request to the appropriate person. The next day we received a letter from the company's DPO, informing us that the cameras were installed in accordance with a regulation making it mandatory for banks to install such security systems. Due to security matters however, the Postbank is unable to provide us with the requested images, nor with the information on storage time or possible deletion. We discussed this matter with the Hamburg office of data protection and were informed that requests on CCTV images do not fall under the definition of personal data for the purposes of access requests as §34 says that only data on a person have to be given out. Images without any relation to name, address or other personal data do not fall under that category and hence cannot be provided. According to the Hamburg DPO's office, German data protection law simply does not allow citizens to view their images if these images are not connected to further data. As such, the Postbank simply does not know who we are simply because we appeared on their CCTV footage. So for reasons of data protection they are not allowed to hand out images of unknown persons via such requests. However, it should be noted that Postbank's negative response did not use this particular justification – they simply argued that security reasons precluded us from requesting our images. A similar request would have been different if on another site our car number plate could have been seen on CCTV and we would ask to access that data. Therefore, our image together with another element of personal data would have renderedusus identifiable. Although this is contradictory to the nature of access rights, this is arguably good practice, as it prevents other people from finding out who was at what place at what time by just stating an assumed presence and requesting that information. However, Postbank's referral to security issues represents a cheap and unnecessary argument, which

[32] A check on the internet provided us with the same information, so that we had little reason to believe that the information was wrong.

fuels new and unneeded suspicions. Given new developments in technology, this regulation may some day be challenged by face recognition software in cameras that link faces to existing databases that are able to identify individuals and link them to other data.

Although our experiences were good, we felt an overall impression that asking for the images of CCTV always raised some sort of suspicion and unease among the people approached. This was also true for smaller shops, where little knowledge exists on installed CCTV, by the often low paid personnel. The shop owners are often not in the shops and therefore cannot answer our queries themselves. We can only speculate about the reasons for that, but would say that CCTV by and large is a contested issue and installing a camera is often accompanied by a guilty or uneasy persuasion, i.e. questions regarding cameras in particular shops or circumstances are met with suspicion because of this existing unease and the knowledge about its contested nature in public debate. However, following a series of opinion polls on the subject, support for public CCTV is mostly said to be relatively high. CCTV in Germany seems to be more of an issue concerning private sites and less so public ones, with the exception of many transport authorities, where many systems operate on a 24 to 72 hour deletion basis. And when researching about CCTV we all should be aware that a camera is not like any other camera or system. So to actually categorise CCTV system, we need to know more about their particular modus operandi, the space they watch, the technology behind it and so forth. In some case a subject access request may make sense, in other cases it does not. Although you do not see this when looking at a camera, we should be careful to simply classify all cameras under the same category.

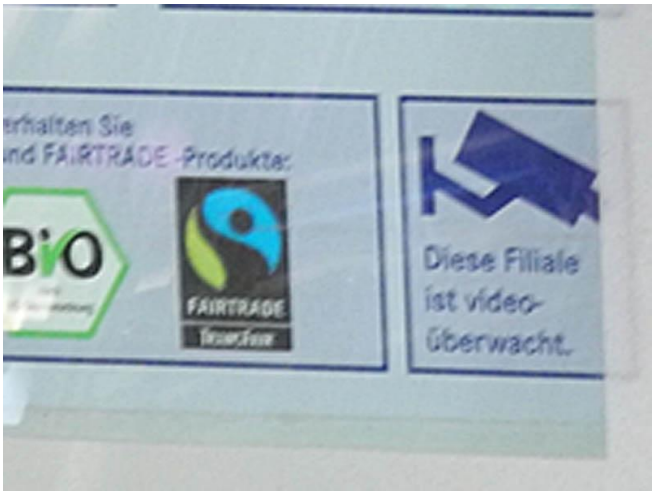
Signage for cameras is rather sporadic, although § 6 (2) BDSG says that cameras have to signposted so that the individual can make an assessment and conscious choice as to accept or evade the CCTV. How this shall work in practice is questionable given that, for example, all banks and ATMs have cameras. The transit authority in Hamburg displays the use of cameras at each door of its trains and busses. Some shops in the station (Dammtor-Bahnhof in this case) have signs, but there is no sign to indicate that cameras are also installed within the station itself. Moreover, some of these signs are difficult to spot. For example, the sign at the drugstore chain is rather small, on a display with other information about the shop, such as fairtrade, bio-products, a family-friendly initiative, or no dogs. Legislation about signs is unclear and it seems that public bodies are under more scrutiny than private enterprises. The smaller you get, the less regulated the use of CCTV seems to be. From previous research we can say that also the smaller a shop is that uses cameras, the less thoroughly these cameras are used. Often they are just symbols or simple systems to meet insurance requirements.

Pciture 1: Sign displayed on a train door

Picture 2: Sign at shop in train station

Picture 3: Sign at newsstand in train station.

Picture 4: Sign at a drugstore chain, Hamburg



Picture 5: Sign at a drugstore chain, Hamburg

Picture 6: Sign at post office / post bank

Concluding remarks

As we have outlined in our report, locating data controllers is generally an easy task with some exceptions. However, it seems to us that the way this is done or what is expected is very much dependent on the local/national context. Some sites are self-evident for the German citizen and work in different ways than the EU directive is describing but crucially, this approach does work. Thus, we do believe that there are cultural aspects of dealing with data protection, of engaging with agents of the state, of trusting institutions or of the overall knowledge of one's rights regarding data issues, some of which we have outlined above, i.e. when explaining the rather widespread awareness of data protection issues and the role of the DPO in German political life. From this research, we may not learn much about the individual and cultural differences in dealing with data on the side of the subject, but on the side of the institutions. As we have described, there are some issues that are quite 'normal' for a German data subject to perform, while others and the awareness of the right to access one's own data might not. There are differences in dealing with these things as well as in our

perception of the procedures, i.e. the way we accept certain procedures or are used to them; also the ways in which data is collected of us. The simple fact that we have an identity card, that is deemed by British as the epitome of the surveillance state, while Germans have accepted this as part of their lives, while being opposed to any form of census may be such a case.

Although the right given to European citizens in the Directive may be applicable for all in the same way, its perception may be not. This does not mean that some citizens live in a less or more democratic state than others. On the other hand we do focus on the reactions of the institutions and probe their democratic behaviour, which may be a better indicator - however there are feedbacks and dynamics involved here that we should address later on, when we analyse the exercise and compare the letters and the outcomes.

SUBMITTING ACCESS REQUESTS IN GERMANY

Introduction

This country report reflects the experiences of submitting subject access requests to 16 different sites within both the public and private sector and across a range of domains. While the results outlined below do not claim to reflect all practices and approaches of organisations in response to subject access requests, the chosen sample is nevertheless reflective of domains with and in which citizens interact on a systematic and consistent basis. Thus, the overall trends observed as part of this research may be indicative of the experiences a citizen may encounter when submitting a subject access request in Germany.

Overall summary

The data controllers and their contact details were easy to locate. This is principally because under German data protection law, any entity - commercial or public - with more than nine employees and which is engaged in data collection and processing has to have a data protection officer (DPO). This in turn means that in practice, letters with access requests could be send to any headquarters with the remark 'c/o DPO' and must in fact be forwarded to that person or department. The experience of this research shows that this does actually happen in practice and there seems to be little worry for the customer, consumer or citizen that a letter - registered or not - is lost. Nevertheless, I opted for registered mail in all cases.

All data protection officers could be found easily via web searches, as could the addresses where to send letters to. Some organisations, especially in the public sector, also provided information on how to access one's data and how to make requests using specific forms and templates. Although I did not use these templates in the first attempts, I often received quick responses from data controllers which helped me. I was therefore guided towards these forms and instructed on the nature of the data processing activities of data controllers and how to access particular data from particular sets of databases.

When searching for public data controllers and in particular for sites concerning law enforcement databases, I came across a website, (*www.datenschmutz.de*) which is (self-entitled) a "resource for the data collection of the security and repression authorities". This organisation provides an online generator for requests to public bodies, such as police, crime records, intelligence services (national and on federal state level) and so forth. Datenschmutz.de is one of many civil rights activities undertaken by citizens concerned with data protection and the state in Germany. So while the website is not official, it represents a bottom-up attempt to help citizens with their rights. The letters generated display the correct legal text for such requests, (which is quite elaborate), and the appropriate addresses depending on which authority the requests are addressed to. I used this generator and was provided with five letters :

- BKA, (federal bureau of criminal investigation) on my personal data
- BKA on data in the Schengen, Prüm and Europol data bases
- Bundesamt für Justiz, that holds the central crime register
- Police Hamburg
- Hamburger Landesamt für Verfassungsschutz (Hamburg office of the internal intelligence service)

Once printed, I just had to sign and send the letters. These letters were sent on 28/08/13 and final information was returned between 04/10/13 and 23/10/13 with some bodies sending mails in between acknowledging my initial letter or asking for an identity proof. All other letters were sent on 04/09/13 and final answers were received in between 11/09/13 (mobile phone carrier) and the 24/10/13 (Microsoft).

	Public/Private	**Site**
1	Public	CCTV in a transport setting
2	Public	CCTV in a government building
3	Private	CCTV in a bank
4	Public	Local authority
5	Public	Police criminal records
6	Public	Europol
7	Public	Border Control
8	Public	Vehicle Licensing
9	Private	Mobile phone carrier
10	Private	Banking Records
11	Private	Credit card records
12	Private	Loyalty card (supermarket)
13	Private	Loyalty card (transport)
14	Private	Ebay
15	Private	Microsoft
16	Private	Amazon

During the course of the research, I held two telephone conversations with data protection officers - one was initiated by myself, following a letter of acknowledgement with a request for further clarification of my initial request; the second call was initiated by Ebay, interestingly calling my mobile number, which I did not provide in the letter. A third call was received from my credit card provider, but I missed it and no further attempt to contact me by telephone was made by the data controller.

Several requests were unknowingly addressed to the wrong person or company. However, I received notice of this and the DPO in each case forwarded my requests to the right person. This happened in the cases of the requests for CCTV in a government builing and CCTV in a transport setting, which was operated by a transport company. In both cases I was notified and did not have to do extra work or renew my requests.

Overall the exercise was rather smooth and significant obstructions were not experienced. However, in many cases little data was retrieved as several responses stated that I was not part of a particular database. This was especially true of the public sector, including police and intelligence data sets. Looking at this from a slightly different perspective however, this may also be a good thing, as it means that not much data seems to be held about me in public authorities' data bases.

Case by case analysis

Public – Facilitative

Local municipality

Within five days of making my request, the DPO of the local council responded and asked me to call her. The reason was that the national law and corresponding section I had quoted in my letter did not apply to this municipality. Instead, the Hamburg data protection law was applicable, and hence a different section. She also asked in the letter that I give more information about my request. I called the DPO and was met with friendliness by a very helpful woman. She explained to me that I had to indicate what data I was requesting, i.e. from what department I want to have the data, as there is no single central data base operated by the local municipality regarding all my data.. I opted for the department of family and youth affairs and the department of construction and environment, because I had approached both of them previously. I re-issued my request on 30/09/13 and received acknowledgement of my new request on 02/10/13 from one of the local authority's departments, and on 04/10/13 from another department dealing with family matters. On 23/10/13, I received a letter giving me information about my stored data. One of the departments advised that it did not have any data on me. The other department had data on me, but did not provide the data itself. Rather, the circumstances in which the data was collected were outlined, i.e. I had an entry on an application for a kindergarten for my sons roughly 12 years ago, which include income, employment and times of care for the children. The second set of data was acknowledged, but fell under a completely different law (which were provided, e.g. § 61 paragraph 2 SGB VIII or § 810 BGB) and relates to support payments for my children and custody rulings after my wife and I divorced. The letter received advised that the data protection laws do not apply here, as the special laws precede federal and local data protection laws and have their own request rules. So I was informed on the data stored about me, but no details were given. However, as I knew about the rulings, I also knew what was in the data and did not file a second request on a different legal basis. I was helped quite effectively and learned new things about the availability of the data.

Police criminal records

Three seperate requests were sent for this site in order to capture every type of data potentially held by policing agencies. The first of these requests was submitted to the police's internal intelligence service. The request was send on 28/08/13 through a letter generated by the www.datenschmutz.de website (see above). I received a reply on 07/10/13 saying that no data or any other files exist about me in their database.

The second request was sent directly to the city's police department on 28/08/13. I did not know what data the police could possibly hold about citizens in general. I received an acknowledgement of my letter on 09/09/13, indicating that a final answer to the request could take up five to seven weeks and asking me not to inquire further in the mean time. On 30/10/13, I received a letter with the data they stored about me, details on the database they stored it in, the legal basis for this data base and my role concerning the data, i.e. legal representative of my son in an accident case, in which my son was involved (as a victim) in 2010. The letter informed me about the time period of deletion (3 years) and the date at which this data set would be deleted (shortly after my request). I was informed about the legal basis of this data storage and referred to the public DPO of the city of Hamburg should I have further questions on this. The address for this DPO was provided. All together, this represents a very good and transparent practice, there was never an attempt to distract me or obstruct my request, but a very helpful and citizen-friendly approach.

The third request was sent to a public sector department which stores criminal record on 28/08/13 and a reply was received on 09/09/13, acknowledging my request, and informing me that the research could take longer and that I should refrain from further inquiries until then. On 15/10/13, I was finally informed that no entries exist about me in the data base of criminal records.

Europol

The request was sent via the BKA as the national contact point to Europol on 28/08/13. After having verified my identification with the BKA (see other entry), my request arrived in Den Haag, Europol's headquarters, on 30/09/13 and was answered on 04/10/13 by Europol, stating that no data about me exists in their data bases.

Border Control

The requests were sent on 28/08/13. It was necessary to send two letters, the first asking for data on the basis of the BKA law and the database INPOL, as well as the German "anti-terror-database", and the second requesting data that may be held under the Schengen Agreement, the Prüm treaty of Europol. On 06/09/13, I received an acknowledgement of my request which asked me to verify my identity by sending a certified colour copy of my ID card to them. In addition, to inquire about possible data in the German anti-terror database, I had to provide justified reason for my request. I did so and provided the following justification: "Due to my academic work on surveillace, urban studies and gentrification, I have had contact with organisations that could have been under scrutiny by the intelligence services. In addition in 2008 I also received very peculiar communications with two persons who stated they were journalists, but who wanted to know more than covered by my scholarly interests. Hence my personal interest in this access request."

The provision of a justified reason is stated in a laws regulating the intelligence services (§ 15 Abs. 1BVerfSchG; § 7 BNDG, § 9 MADG), which were provided. The law on data protection provides the possibility of such restrictions.

The acknowledgement letter was accompanied by a six page document which informed me about what databases existed, what their purpose was and what might be stored in them. It also informed me about the nature of various forms of data - open and closed - and the ways in which I may access one or the other (the latter rather not really). Three of the six pages were addresses of all police authorities in Germany that cooperate within this legal framework, thus providing me with an extensive list of contact addresses for police authorities.

In order to satisfy the identification requirements, I obtained a verified copy of my ID card from the local council‘s citizens service centre, providing my own copies and my ID card. I paid 3.5 Euros for this service and sent the documents to the BKA with an accompanying letter on 18/09/13. The final answer from the BKA came back on 01/10/13, explaining that none of the data bases held data about me, and that my request concerning Europol had been forwarded to them (see above). Although I had to provide further data and an ID copy for my request, this was clearly explained to me and the legal backgrounds as well as the process was quite transparent. It did not take long and throughout it seemed that my rights as a citizen were taken very seriously. The responses were I received reflected this feeling. The BKA even sent back the ID copy, so I could use it for other purposes if necessary.

Vehicle Licensing

With a letter on 04/09/13, I requested access to my data at the national vehicle licensing authority. On 11/09/13, my letter was acknowledged and further information was requested by the authorities. As the authority maintains various databases, which have different purposes and different legal bases, I was asked to specify my request and I was given information on the data collection activities of each database and what I needed to do to access my data. This information was quite extensive and included the possibility to access the data online, if I had a card reader, an ID card app and the latest version of the ID card (issued after 1/11/2010, which I do not). I was given information on the template via which one can request data from one of the databases (VZR) and the details required from me to request my data from the three other databases (i.e. name, first name, date of birth, place of birth and my address). I also had to include a copy of my ID-card and sign all requests.

I sent those requests on 18/09/13 and received the requested information at different intervals on 24/09/13, the following day on 25/09/13 (two) and finally on 01/10/13. Only one database held data about me - the central vehicle registry - which held data on my current and previous cars. I was also advised that data older than seven years is deleted in any case (except for the current car). Interestingly, I was not listed in the registry of driving licences, because I obtained my licence prior to 1999 and have not changed the document yet - to a newer, more modern issue, as diving licences have no expiration date in Germany. Hence a record on my licence is only stored at the issuing authority, i.e. the traffic department of the city of Hamburg, where I obtained the licence in 1986. The fact that there is no interlinkage is interesting and demonstrates the highly restrictive data protection laws regarding data sharing in many field of the public sector are in practice.

Overall, the examples above show that data access requests are relatively easy in the public sector. Public authorities have shown a good practice regarding compliance with the requests and the transparency of their decisions. Where there were further demands on me to provide

extra information such as a certified copy of my ID card, this was made clear and the process was facilitated as much as possible. While this may put some extra burden on the requesting person, it seemed generally feasible and unproblematic to me. The legal basis of decisions are explained to the data subject, including when full disclosure of some information is not possible. So in case I wanted to look up the data stored about me at the local department of family and youth, I would have the relevant legal departments available to help me. The fact that I could call the data protection officers of the respective bodies generates some form of trust and does away with the image of the powerful, but invisible bureaucracy that acts, but cannot be questioned.

However, an odd feeling remains that I will never have the possibility to fully understand the pathways my data takes within and between different public bodies and how this data is processed. Much of what I learned is what I knew anyway. The interesting question therefore becomes whether this is truly all the data held about me, or am I only told so much? Data access requests are a good measure to increase trust, but necessarily remain a weak instrument, if not handled fairly on the side of the public bodies.

Public – Restrictive

No significant examples were found in this research of restrictive practices in the public sector.

Private – Facilitative

Banking records

The request was sent on 04/09/13 2013 and I received their response on 23/09/13. I was not notified as to the progress of my request in between, but I was given the data that was stored about me, including the date when they requested a scoring analysis from SCHUFA and including the number of my ID card. I wondered why they did not give me the data of my account itself, such as all movements on the account, but I assumed this was because I can access this myself anytime I want to via my own banking records. While the omission of my banking transactions may therefore appear to be incomplete, I did not regard this as so since all this data is already available to me. The bank's response therefore avoided any unnecessary repetition and seemed to me to be reasonable.

Credit card records

The request was sent on 04/09/13 and replied to on 25/09/13. On 17/09/13, I received a call from the company's DPO, but missed it. No further attempt was made to contact me. No voice mail was left, but when I called the number which had appeared on my phone, I got to a voicemail in an office at the company. I did not try to call this number again and in any case the letter arrived in my mailbox shortly thereafter. When the reply came, I was surprised not to find any data enclosed, but instead a letter explaining where to find my data, (apparently with the issuing bank). This is apparently because the company does not process my data, but merely gives out licences to the banks, who then process the data themselves and deal with the credit process. The DPO advised me to contact the bank which issues the credit card and request my data. I did not inquire any further, but was surprised as I thought Mastercard would handle my credits records themselves.

Mobile phone carrier

The request was sent on 04/09/13 and I received a reply on 11/09/13 - a week later. This was the fastest response in the sample. The letter contained the stored data, telephone numbers, SIM card number, customer matchword, addresses, account number and so forth. However, it did not contain my connection data as I had requested in my letter. However, I was told why this was so: I had not opted for a bill with this data, so they are not obliged to provide this data in retrospect. The relevant legislature was cited, which is Telekommunikationsgesetz §§96, 97, 99. In addition I was informed that the company does not give out data to third parties, except in the case of debt collection, which is also regulated in the TKG § 97. They also explained that they had contacted credit rating agencies when I signed the first contract with them and told me which ones hold my data about my telephone contracts. Although the information is transparent, it leaves me unsure whether there is data about my phone use (such as geo-locational data), which I could use or which somebody else could use. As such, the response received felt somewhat incomplete and I was unable to determine with any certainty whether I had received complete disclosure of my personal data. The problem of unknowables therefore arises here which pertains to some extent to the asymmetry of power between data controllers and data subjects insofar as it is very difficult in some cases for individual data subjects to know if the entirety of their data has been provided.

Loyalty Card (supermarket)

The organisation is a medium sized company (drugstore) in Hamburg, which issues a loyalty card that is quite popular in Hamburg. This is arguably due to with the image of the company, its charity activities and its role as a "good" drugstore in comparison to others, who do not pay their employees enough (among other things). This reputation was upheld when I received an email by the DPO of the company two days after I sent the letter on 04/09/13. I was advised that their external service provider for the loyalty card was informed and the request was being processed. I received another email on 13/09/13 informing me that the requested data had been sent via registered mail to me. The letter I received, strangely carrying the date 20/09/13, held all information on my purchases between 10/07/13 and 12/09/13 (the period during which I have owned this card), the original application for the loyalty card (a copy thereof) and a letter explaining a few things about my membership. I was informed that I was registered as a "commercial denier", meaning that I was not to be sent personalised advertisements, as per my preference on the original application. I was informed about the reasons why the company issues loyalty cards and what they do with the data, i.e. organise the layout and design of shops. I also learned that the company has installed an audit of its data protection practices and will be certified in this regard by 2014. The impression of the "good" company was upheld, however the data provided was what I essentially already knew and I could not find any information regarding deletion of data, other than to withdraw from the loyalty programme altogether.

Loyalty Card (transport)

The request was sent on 04/09/13 and acknowledged on 11/09/13. The final information was received on 20/09/13, including a data set from the database. This included my addresses between 2003 and today (including the exact period), date of birth, email and a very old telephone number (previous work number from around 10 years ago). It listed the products I have been purchasing since 2003, i.e. a mileage card for the German rail, that is issued on an annual basis and renewed every year. The data also listed a credit card which does not exist anymore - I pay the card annually by invoice - and my current point status in the bonus point programme, to which I signed up. However it did not reveal the travels I booked with this card and for which I collected the appropriate points. This may be because this data is

available to me via the company's website by accessing account. Alongside each type of data, it was mentioned who the source of the data was - myself. Although the process was easy, transparent and quick, the data seemed to be incomplete and indeed I know that more is stored about me. What I do not know is whether that kind of data is only visible to myself or open to the data controllers as well. This may be seen as an asymmetry of power, in as much the data controller decides what to disclose to me. However, if it is data that I can access simply by going to my account and checking my bonuses and travel history classifying this omission as an incomplete disclosure by the data controller seems unduly harsh. Rather, issues of trust actually emerge when thinking of whether I am told all possible uses of the data and any possible third-party availability.

Microsoft

The request was sent on 04/09/13 and acknowledged on 18/09/13 by mail. I was asked to provide a proof of my identity by sending a copy of my ID card. On 01/10/13, I received an email telling me that my request was not processed in Germany and the request had been forwarded to the US headquarters - my initial letter went to the German head offices in Munich. On 24/10/13, I received a letter, stating that no information of or relating to me were held by Microsoft. The letter came from the German office and they referred to information they received from the headquarters of MS, presumably located in the US. As I am a registered user of some of their software I thought I must have left a trace in their data base, but according to this request I have not. This may spur thoughts about bad practice, unknowables or even conspiracy. However the letter also states that if I had registered under a different email for instance, they would not be able to find the according data for the email that I provided. All in all a good practice, but one that still leaves some questions unanswered.

Ebay

The letters concerning Ebay were sent on 04/09/13. Two letters were sent as one was sent to Ebay in Luxemburg and one to the overseeing data protection officer of the state of Brandenburg with a remark in each letter about the fact that I had sent a copy of the same letter to another address. This I thought was a viable measure, as Ebay has a German headquarters and therefore is subject to German law. However I wanted to address it to Ebay directly, which is why I chose the Luxemburg address. In addtion I read in a forum that this is a good strategy to make sure the request was taken seriously and as an insurance for myself. On 16/09/13, I received a phone call from a German speaking woman, presenting herself as being from the complaints department of Ebay and wanting to inquire further about my complaint. I had to tell her that I did not have a complaint, but simply wanted to exercise my right to submit a subject access request. I had a long and friendly talk with the lady, who revealed herself to be a German national working for Ebay in Ireland. She advised me on the type of data Ebay keeps, what is deleted and according to what retention periods and so forth. It was informative and very helpful. She assured me that all data would be sent to me as requested. The information arrived on 20/09/13 in the form of an email. This included very basic information like name, email, address, date of birth and mobile phone number. The email informed me that Ebay also stores the data on my purchases - however, the lady I had spoken to on the telephone told me that different data will in fact be deleted. She explained that purchases will be securely stored for 2 years and emails for 1 to 2 years. However when you close an account, 180 days thereafter all data will be deleted. As such, the telephone conversation I had and the email I received addressed slightly different types of data and how this data is processed.

Private – Restrictive

Amazon

Amazon may be considered as an example of somewhat restrictive practice in the sample. After my initial request, which was sent on 04/09/13, I received two emails which did not directly acknowledge my letter and request. Instead, these emails referred to data protection issues in general. The first email, received on 13/09/13, said that if I wished for my account to be deleted, it would have consequences for my data, i.e. it would be ultimately lost, together with the account etc:.

Letter dated 13/09/13:

> "Message from Customer Service,
>
> Hello, we accept your decision. An important tip - closing your account has the following consequences: ..... [followed by a list of things that happens to my account]. yours friendly"

I answered the mail, saying that I did not request such a procedure, nor did I ask for my data to be deleted. The tone of their email seemed to be a warning and I thought it inappropriate.

The second email received on 17/09/13 was merely a direct quotation from the company's data protection policy (see below), which could also be found on their website, signed by a different person than the first email:

Letter dated 17/09/13

> "Message from Customer Service,
>
> Good evening, data protection is important at Amazon's. We have published our data protection on our website, which shows how we store and deal with the information of our customers. Thanks for your efforts and a lovely evening
>
> yours friendly."

I again responded in a friendly manner, indicating that this was once again not what I had asked for. On 21/09/13, I received an email addressing me in person, saying that my request („thanks for your fax" - I never faxed anything) was being processed and that I would have my data in the mail very shortly. The email was very short, telling me that I would receive my requested data by 30/09/13 and was signed by a third different person. They thanked me for visiting Amazon. Overall the experience did not generate trust, but suspicion and I did not feel like I was being treated as a serious customer. Amazon also seemed not to care or even be aware of about the ongoing thread of communications (fax, deletion of account, nature of my request). The emails seemed to be warning me or keeping me from further pursuing the request of my data. The image that emerged was that of a super-sized company, where the individual customer never gets through to the important and correct person for the request - unlike all other bureaucracies I encountered during my requests.

The letter with the information printed out carried the date 20/09/13 (and came from the German headquarters) and contained 46 pages of information of my purchases, and my addresses - going back 13 years when I started using Amazon, albeit under a different account (and mainly amazon.co.uk at the time, as I was living in the UK), which I renewed in the meantime. It was not clear whether the emails previously received were connected to my

request. Broadly speaking, I assume that they were intended to distract me from the request, warn me and maybe discourage me from making the request, or pursuing it any further. I found this an irritating, impersonal practice on behalf of Amazon, as part of which the company lived up to my (low) expectations. I was even more irritated by the fact that Amazon does not delete data - not even addresses that are old - but seems to transfer data from one service (UK) to another (Germany) together with the account data.

Given the difficulties prior to submitting the request described above, I was particularly surprised when the actual data arrived given its coverage. What did not arrive however, was any information regarding possible credit scoring practices or how my data is treated by Amazon in particular. It remains unclear therefore, whether Amazon keeps a score of me and rates my activities in any way.

In line with this is the latest decision by the German supreme court (Bundesgerichtshof, not constitutional court[33]), which ruled that the major scoring company in Germany - SCHUFA - does not have to reveal the criteria for the overall scoring, merely the data such a decision is based on. Credit rating decisions themselves are visible anyway, but not the process by which such decisions are arrived at. The main argument in the case was that business secrets have to be secured by not revealing the criteria and weighting of particular aspects or information.

CCTV

I made only three requests for CCTV images, because I knew after a first test run that CCTV images do not have to given out according to German law, due to the lack of personal relation of the data to the person - see phase 1 report, where I elaborated on this issue. I made two more requests with the same results, albeit with different arguments on the side of the companies - one being the transit authority of Hamburg, the other being my bank.

I favour the idea of deleting data after a short period of time, (i.e. 72 hours in Hamburg) if nothing occurs for which such images might be needed. I think this represents a good practice, if it can be ensured that no misuse can happen under such a system. Interestingly however, during the research the responses of data controllers in CCTV sites did not refer to the correct legal bases when denying the disclosure of CCTV footage. Instead, other rationales were used and are outlined below.

CCTV in a government building

In reply to my request for CCTV footage, the organisation wrote:

> *"I kindly ask you to understand that we can not give any information regarding the security technologies in our branches. Complying with bank laws we have to install optical surveillance. We point to the fact at the entrance through signage* [which they do]*."*

CCTV in a bank

In this case, I received a letter denying me access to the CCTV footage. The letter advised that CCTV is there to help minimise the dangers of debit card fraud, vandalism or robbery of customers (using ATMs). It further outlined that § 28 BDSG (data protection law) allows the data controller to record and use the images, because they have a justified interest to do so.

[33] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=66583&pos=1&anz=17

The data controller argued that there is no justified interest on behalf of customers which overrides the interest of the data controller to make such recordings illegal. The letter also sought to assure me that they handle all data with care and they follow the law in using or providing the data to third parties such as the police. If nothing happens, all data is apparently deleted after two weeks.

CCTV in a transport setting (subway)

In advising that the footage could not be disclosed, the data controller outlined the following reasons:

> "*We have CCTV installed in our subways since 2004, a procedure that was closely realised together with the Hamburg DPO at the time. Recordings will be stored for 24 hours and overwritten, if no reason occurs to view the data. Such reasons could be police investigations, vandalism or other. In your case I can therefore assure you that the recordings have already been deleted. Nonetheless, even if we would have had the data, we would not have given it to you, as we are not allowed to give the data to other parties then the police."*

Since I had sent the letter weeks after I was on the subway, this made sense and overall as stated above, deleting the data is a very good practice.

While German data protection law allows data controllers to deny access to CCTV footage, it is noteworthy that none of the data controllers who denied my requests referred to the correct legal articles for such denials. Instead, they relied on a variety of reasons for not disclosing the footage, all of which are common sensical but are technically not the main legal justification for not allowing data subjects to request CCTV footage. This shows that data controllers of CCTV systems are perhaps unclear as to why they are entitled to deny data subjects access to CCTV footage.

Concluding thoughts

As this report has shown, the process of access requests in Germany seems fairly easy to achieve. Of the 18 requests submitted, only one seemed to be obscured by ambiguous emails (Amazon), while the request itself was answered within three weeks. The overall information on legal issues received was transparent and at a good level of expertise. While the approach I took was that of a lay person's, it has to be said that knowing about the possibility of such requests and then in fact requesting the data, renders one a semi-expert. Where extra information, such as proof of identity or else, where requested, the reasons where transparent, but it was clear that such requests for verification should not discourage data subjects from pursuing their requests as they did not seem adverse. Comparing public and private entities, it seems that the private sector bodies were slightly more defensive in their language than their public counterparts. I was surprised by the compliance and readiness to provide information, although it has to be said that the information itself was often disappointing. There was not much that I did not expect to see or that I did not already know - as I was the one providing much of this information in the first place. What was potentially missing was information about analytical uses of the data and the possible ways of sharing data, which were foreclosed in many of the data protection statements, but which happens through legal loopholes anyway, .e.g. the make-up of business consortia which then would not count as third parties. As for public bodies, it remains unclear which linkages exist between different bodies - e.g. police, local councils, transport authorities (public-private entity) and so forth. Do networks of data sharing exist or not? There is little transparency on this point. As such, the data alone

is not much of a story, but the assemblage of the data through different bodies - public and private – is perhaps more noteworthy. Having said this, I have to admit that the possibility of accessing one's data alone is a big step forward in state-citizen relations (concerning public bodies). Citizens now have the possibility of engaging in dialogue with the state and actually talk to the bureaucracy as part of a guaranteed right. German data protection law seems to equip citizens with a strong tool with which to do this, backed by a civil right and a strong public debate. The latter is still necessary as data protection is neither self-evident, nor are the DPAs so powerful as to act as legally intervening bodies with executive rights in particular cases.

SIGNIFICANCE OF FINDINGS - GERMANY

Throughout the duration of the research undertaken within this project, the question remains whether access rights are a truly powerful tool in the hands of the citizen or a mere placebo. It certainly has changed relations between customers/citizens and business/state, but only accompanied by a decade of public debate and public (and media) awareness of the subject itself in Germany. I would doubt that the law on its own would have that effect. Whether having all those data or no data whatsoever, the question remains whether what is disclosed is really all that is held about me or whether I am not told the truth. As a result, the following questions arise:

a) did I receive all the data held about me?

b) did I receive full disclosure about how my data is shared or used further?

As data is a very elusive and mobile phenomenon, storing, sharing, protecting or deleting data is very dependent on the persons doing so and following due process (or algorithms programmed to do the job correctly), but always vulnerable to misuse. Given that some form of data is always needed in a bureaucratic society, the question becomes how much of this data is necessary to collect, what kind is required and for what purposes? Moreover, are there ways to regulate this in the first place? Data protection should also be data avoidance. To fantasize about a data-less society with no computers processing is out of question. So having regulations that are followed and can be scrutinized and audited seems to the only way of controlling such activities and thus empowering the citizen. The difficulty is to find a way between the rights of privacy and informational self-determination of the individual, the interests of the state to provide services, fairness, equal rights and security and the interests of companies to do their business. Clear laws and the will to follow it on all sides, supported by a strong public interest seem to be the only guarantee of making this right a right for the citizen.

However, if one suspects otherwise and feels that there is always something the state or firm does not tell, there is no way out, as no one will ever know. Something that also protects the citizen from too much state intrusion after all.

References

Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0015 (last accessed 20 December 2013)

Biermann, Kai: "Was Vorratsdaten über uns verraten", in Die Zeit Online, 24.2. 2011, http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz (last accessed 20 December 2013)

Bundesgerichtshof - http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2ef8cefa03b7d0493f54c1bc71ee0a53&anz=1&pos=0&nr=66583&linked=pm&Blank=1

Bundesverfassungsgericht, decisions volume 65

Census results: https://www.zensus2011.de

Federal Constitutional Court, (Bundesverfassungsgericht), 1BvR 256/08 of 2.3.2010, paragraph no. (1 - 345), judgement of 2 March 2010, available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (last accessed 20 December 2013)

Federal Constitutional Court, (Bundesverfassungsgericht), http://www.bverfg.de/pressemitteilungen/bvg10-011en.html (last accessed 20 December 2013)

Federal Data Protection Act (BDSG), in the version promulgated on 14 January 2003; http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile (last accessed 20 December 2013)

Federal Data Protection Act (BDSG): http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/BDSG/BDSG_node.html (last accessed 20 December 2013)

German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 2378/98 vom 3.3.2004, http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html (last accessed 20 December 2013)

German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), judgment of 27 February 2008, available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html (last accessed 20 December 2013)

German Federal Constitutional Court (Bundesverfassungsgericht), BVerfG, 1 BvR 1299/05, order of 24 January 2012, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg12-013en.html (last accessed 20 December 2013)

Gieseke, Jens: Die Stasi, München, Pantheon, 2011

Hannah, Matthew, "Dark Territories in the Information Age. Learning from the West German Census Controversies of the 1980s", Farnham, Ashgate, 2010

Hoss, Dennis, "Auskunftsrecht des Betroffenen aus § 34 Abs. 1 BDSG in der Praxis: wirksames Instrument oder zahnloser Tiger", Juris, RDV 2011, 6-11

http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2ef8cefa03b7d0493f54c1bc71ee0a53&anz=1&pos=0&nr=66583&linked=pm&Blank=1 (last accessed 14 April 2014)

http://www.datenschutz.de/recht/gesetze/ (last accessed 20 December 2013)

https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf
Killian, Wolfgang, "Germany"; James B. Rule and Graham Greenleaf, "Global Privacy Protection. The first Generation". 2008, pp.80-106

Mallmann, Otto, “Zum datenschutzrechtlichen Auskunftsanspruch des Betroffenen”, GEWERBE ARCHIV (GA): Zeitschrift für Gewerbe- und Wirtschaftsverwaltungsrecht Nr. 9 vom 09. September 2000, p. 354

Papier, Hans-Jürgen, “Verfassungsrechtliche Grundlegung des Datenschutzes”; Jan-HinrikSchmidt and Thilo Weichert, “Datenschutz”, Bonn, Bundeszentrale für politische Bildung 2012

Roßnagel, Alexander, Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München, Beck, 2003

Schmidt, Jan-Hinrik and Thilo Weichert, “Datenschutz”, Bonn, Bundeszentrale für politische Bildung 2012

Supreme court ruling on information access to scoring practices by consumer: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=66583&pos=1&anz=17

von Lewinski, Zur Geschichte von Privatsphäre und Datenschutz - eine rechtshistorische Perspektive. Jan-Hinrik Schmidt and Thilo Weichert, “Datenschutz”, Bonn, Bundeszentrale für politische Bildung 2012

Worms, “Beck‘scher Online Kommentar”, Stand 1.5.2013, Edition 4, BeckOK BDSG § 19

Zurawski, Nils. Consuming Surveillance: Mediating Control Practices Through Consumer Culture and Everyday Life, in: Jansson, André / Christensen, Miyase (eds.) Media, Surveillance and Identity, New York u.a. 2014, Peter Lang.

Zurawski, Nils: Local practice and global data. Loyalty cards, social practices and consumer surveillance – Sociological Quarterly, Volume 52, Issue 4 (winter) 2011

List of Abbreviations

BDSG - *Federal Data Protection Act (*Bundesdatenschutzgesetz*)*

BKA - Bundeskriminalamt (Federal office of Criminal Investigations)

BVerfGE - Federal Constitutional Court, (Bundesverfassungsgericht)

BvR - Bundesverfassungsrichter (Judge of the Consitutional Court)

CCTV – Closed curcuit Television

DPA – Data Protection Authority

DPO – Data Protection Officer

ECJ - European Court of Justice

EU - European Union

GG - Grundgesetz (German Constitution)

ICD Code - International Statistical Classification of Diseases and Related Health Problems - issued by the WHO

SCHUFA - Company name of German credit scorer, used to be and is derived from: Schutzgemeinschaft für allgemeine Kreditsicherung (Protection company for general creditworthiness)

SGB - Sozialgesetzbuch (Collection of Laws on social and welfare issues)

TKG – Telekommunikationsgesetz (Law on telecommunications)

VZR -Verkehrszentralregister (Central traffic registry)

WHO - World Healh Organisation