Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

German national report
EDRi

Bogdan Manolea and Meryem Marzouki
European Digital Rights
December 2009

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH,EDRi,AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

General synthesis

I.1. Legislation regarding privacy

Germany has a unique European development of the right to privacy and its interpretation by the Constitutional Court that had a major impact in the data protection legislation and, to some extent, also to other European countries' data protection legislation.

The privacy of communications was included in the German Constitution in article 10[1] in its version adopted in 1949. But the German Constitution (Grundgesetz für die Bundesrepublik Deutschland) also included in the first articles of the text (Articles 1(1) and 2(1))[2] the personal rights to freedom (Persönlichkeitsrecht).

These personal rights to freedom have been interpreted by the German Federal Constitutional Court as a right of "informational self-determination". In a landmark decision from 1983[3] the Court has considered as unconstitutional some provisions of the German Census law that allowed personal information to be gathered by the Federal Government and shared with the Local and Lander Governments. The court noted that the technical developments make possible for the automated data processing to create a complete personality profile. Thus the court pointed out: "Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them."

The German Constitutional Court was consistent in this approach also in newer cases. Thus in the *Großer Lauschangriff Case* (2004), the court has considered[4] that acoustic surveillance of the

---

1 Article 10 (1) The privacy of correspondence, posts and telecommunications shall be inviolable.(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

Official Translation available at http://www.bundestag.de/interakt/infomat/fremdsprachiges_material/downloads/ggEn_download.pdf

2 Article 1

(1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.

(...)

Article 2

(1) 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.

3 Federal Constitutional Court (Bundesverfassungsgericht) decision of December 15, 1983, reference number: 1 BvR 209, 269, 362, 420, 440, 484/83.

4 BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. (1 - 373), available at http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html

home by the state was constitutionally prohibited and described the home as „ last refuge for the development of one's personality and preservation of one's dignity."

Even more recently in February 2008 the Court has issued [5]a new landmark ruling, constituting a new "basic right to the confidentiality and integrity of information-technological systems" as part of the general personality rights stipulated in the German Constitution. The reasoning goes: "From the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use follows a need for protection that is significant for basic rights. The individual is depending upon the state respecting the justifiable expectations for the integrity and confidentiality of such systems with a view to the unrestricted expression of personality."

Information-technical systems that are protected under the new basic right[6] are all systems that "alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality."

The debate on the privacy and computers started in Germany in the 1960s and the first data protection legislation was adopted in the Lander of Hesse in 1970, that foreseen also the creation of a Data Protection Commissioner. After long debates in the German Parliament and in the public arena, the German Federal Data Protection Act (Bundesdatenschutzgesetz or BDSG) was enacted in January 1977. It was then revised several times during the years, with a major review in 2002 in order to comply with the European Data Protection Directive. Another extensive modification was made in 15 November 2006.[7] The general purpose of this Act is to protect physical persons against the mishandling of their personal data. The Act covers[8] collection, processing and use of personal data by public federal authorities and state administrations (as long as there is no state regulation and insofar as they apply federal laws), and by private bodies, if they rely on data-processing systems or non-automated filing systems for commercial or professional use.

The BDSG was amended three times in May-July 2009, with the new modification entering into force on 1 September 2009.[9] One of the major changes is the inclusion of mandatory data breaches notification as a requirement for data controllers.[10] They must notify the data subjects

---

5 Constitutional Court Decision (BVerfG, 1 BvR 370/07) available at http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

6 More info about the decision in EDRi-gram 6.4, 27.02.2008 - Germany: New basic right to privacy of computer systems - available at the http://www.edri.org/edrigram/number6.4/germany-constitutional-searches

7 The latest version of the Act can be found in English and German on the Federal Data Protection Authority website available at http://www.bfdi.bund.de/cae/servlet/contentblob/411288/publicationFile/25384/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

8 For a more detailed overview of its provisions and secondary legislation, see Privacy and Human Rights 2006 – Germany available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559535

9 The amendments and the consolidated text can be found (only in German) at http://www.cms-hs.com/CMS_BDSG-Novellen_I-III_Synopse_090710

10 For a more detailed analysis, see Mauricio F. Paez and Jörg Rehder - Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement , 2.11.2009, available online also at http://www.mondaq.com/article.asp?articleid=88440

and the DPAs of any unauthorized access or unlawful transfer of personal data, if the incident "threatens significant harm" the rights of the subjects. The law does not define the „significant harm", but limits the notification to the cases when sensitive data or credit-card or banking data has been mismanaged. The new changes also implement a higher safety for the company's internal data protection officer, that may not be fired in any circumstance. Also the companies need to provide them with continuous education of data protection issues. The law also allows the use of external data protection officers. The new adopted provisions increase the powers of the DPAs that can order the private sector actors to improve the compliance with the BDSG, including prohibiting companies in dealing with personal data.

All the German Landers[11] have each adopted legislation in the field of data protection, that implements the European Data Protection Directive. The Landers legislation covers regional public administration, but also the compliance of the private companies with the BDSG.

I.2. Data Protection Authorities

The German Federal Data Protection Authority, as set up by the BDSG is the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz). The Authority is considered an independent federal agency and publishes a semi-annual report. The Authority is managed by a Commissioner who is elected by the German Parliament (Bundestag) for a five-years term, based on the proposal of the Federal Government. The Commissioner is independent in his work and does not receive instructions regarding his work. His main attributions are foreseen in the BDSG. He checks the compliance of the federal administration with the Federal Data Protection Act, but has also the possibility to be involved in legislative procedures by giving opinions and advices on the texts that might affect citizen's privacy.

The specific Lander Data Protection legislation foresees a Commissioner in every Land, that has to implement the regional legislation. Therefore there are also 16 Regional Data Protection Commissioners in Germany.

There is a close collaboration between the Federal Commissioners and the Regional Commissioners that meet on a regular basis to discuss common interest issues and to adopt resolutions of the National Data Protection Conferences.[12]
They also meet regularly in what is called the Düsseldorfer Kreis[13], which is an informal association of the major data protection regulators in Germany, that deals with the application of the data protection principles by the private sector.

The Federal DPA is also involved in privacy awareness activities[14], including organizing events for celebration of the European Data protection day or the local celebration of 25 years from the

---

11 The Landers legislation and their Data Protection Authorities can be accesed via the Federal Data Protection Authority website http://www.bfdi.bund.de/cln_118/EN/AdressesAndLinks/Landesdatenschutzbeauftragte/Landesdatenschutzbeauftragte_node.html

12 Publicly available at http://www.bfdi.bund.de/cln_118/EN/PublicRelations/Publications/functions/NationalDSK_table.html?nn=410160

13 See its recommandation adopted at http://www.bfdi.bund.de/DE/Entschlie%C3%9Fungen/DuesseldorferKreis/DKreis_node.html

Census decision of the Constitutional Court that has created the related jurisprudence on information self-determination. The Federal DPA also organized yearly conferences on hot topics related to privacy (the issues of search engines in 2007 and the telecom- related databases and the revision of the e-privacy directive).

Some Lander DPA are active in the field of privacy awareness, starting with campaigns on different hot subjects, guides on how to protect the privacy[15] and participation in European cross-sectorial projects on privacy.[16] It is also important to note their involvement in creating and supporting Privacy Enhancing Techniques. From 2001 the DPA from Schleswig-Holstein has been involved in a joint project[17] with the Dresden University of Technology in order to create an open-source software that could enable every user to protect his privacy on the Internet. The client software JAP[18] provides anonymous and unobservable communication in the Internet. JAP runs on the JAVA platform and is easy to install and use to enable greenhorns among Internet users to protect their privacy.

The same DPA from Schleswig-Holstein has been active in promoting best practices in the field of data protection at the European level, through its extensive implication in the EuroPriSe - the European Privacy Seal project, as a project leader together with a consortium of nine European partners.[19]

I.3. Other Campaigns

Germany has one of the most active civil society responses to the current problems related to privacy and data protection in the digital age.

To name just a few of them, EDRi-member FoeBuD has been active in protesting since 2003 against the usage of RFID[20] without proper security safeguards or information to the customers. Also in 2004, when Metro started[21] a trial project to introduce a new cashing and customer convenience program at their Metro Future Store with Radio Frequency Identification (RFID) chips, FoeBuD discovered that the cards could not be deactivated and that the RFID devices were also inserted in the personal customer shopping card without notifying consumers.
FoeBuD was also warning against the improper usage of CCTV[22], based on the projects deployed in North Rhine-Westphalia.

---

14 For details see chapter 15 of their Annual Report, page 145 and following. Report also available online at http://www.bfdi.bund.de/cae/servlet/contentblob/567076/publicationFile/31926/22TB_2007_2008.pdf%3Bjsessionid=0D1A0001830C983BA8DD73F21C7054F2

15 See the Rheinland-Pfalz DPA Guide on using Social Networks on the Internet - http://www.datenschutz.rlp.de/downloads/oh/oh-Selbst_DS_soziale_Netze.pdf

16 See for example the Schleswig-Holstein DPA participation in Prime Life Project or RISER. More info at https://www.datenschutzzentrum.de/index.htm

17 Presentation of the project can be found on their DPA webpage (only in German)- https://www.datenschutzzentrum.de/projekte/anon/ For an English presentation see ERCIM News No.49, April 2002 An.on - Privacy Protection on the Internet - by Hannes Federrath available at http://www.ercim.org/publication/Ercim_News/enw49/federrath.html

18 Project at http://www.anon-online.org/

19 For more details about this project, see https://www.european-privacy-seal.eu/

20 The campaign page at http://www.foebud.org/rfid/

21 See more info in the Privacy And Human Rights Report Germany 2004 available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83513

22 See http://www.foebud.org/video

Another EDRi-member Netzwerk Neue Medien, has been active in protesting and present statements against biometrics and RFID usage.

Several NGOs have organized since 2000 the German Big Brother Awards[23] in order to show the worst companies, organizations and individuals that have undermined the human privacy and the protection of personal data.

Starting with the new European Data Retention Directive that needed to be implemented also in Germany and with other actions by the German Government that have increased the surveillance on the German citizens (such as the online computer searches, increased domestic Internet intelligence powers, etc) the civil society actions have passed on a new level.

A special group – called Working Group on Data Retention (AK Vorrat) - was formed as an association of civil rights campaigners, data protection activists and Internet users to fight against the data retention law in Germany. After an intensive campaign against the draft law and after its adoption by the German Parliament, the group has challenged [24]the law before the Federal Constitutional Court, backed by 30 000 complainants. The court already issued a preliminary decision on 19 March 2008, considering[25] that parts of the act are unconstitutional pending review. The final decision of the Court will be taken on 15 December 2009.

More than100 civil liberties groups, professional associations, unions, political parties and other organisations have joined together to organize[26] on 11 October 2008 the first worldwide protests against surveillance measures such as the collection of all telecommunications data, the surveillance of air travellers and the biometric registration of citizens. These were held on under the motto "Freedom not Fear - Stop the surveillance mania!" in at least 15 countries citizens. Here the participants demanded a cutback on surveillance, a moratorium on new surveillance powers and an independent evaluation of existing surveillance powers. The greatest protest march against surveillance in Germany's history took place in Berlin with over 15,000 protesters marching in a rally that ended at the Brandenburg Gate. A similar event was also held on 12 September 2009, when 25 000 people were present in the streets, under the same motto as in 2008.[27] The event was replicated also outside Germany with different type of actions for data protection and against online surveillance.[28]

I.4. Summary of files

In the current study, based on the common matrix grid established in the meeting with all the other Project partners, we will detail in special files the following issues:

- **Mobility and transportation**

23 See more info at http://www.bigbrotherawards.de
24 EDRi-gram 6.1 - http://www.edri.org/edrigram/number6.1/germany-data-retention
25 EDRi-gram 6.6 - http://www.edri.org/edrigram/number6.6/germany-data-retention-decision-cc
26 See EDRi-gram 6.20 - International Action Day "Freedom not Fear" – 11.10.2008 - http://www.edri.org/edri-gram/number6.20/freedom-not-fear-international-day
27 For more info see the webpage of the event at http://wiki.vorratsdatenspeicherung.de/Freedom_Not_Fear_2009
28 For an overview see EDRi-gram 7.18 http://www.edri.org/edri-gram/number7.18/freedom-not-fear-2009

The car plates recognition systems have been selected as a topic to be highlighted due to the recent German Federal Constitutional Court Decision that has declared as unconstitutional several provisions from the two States (Hessen and Schleswig-Holstein) in this field. Also, the development of the implementation of car plates recognition system has differ a lot from state to state, making the local situation more interesting in terms of practical application and legal framework.

- **Biological identity**

The biometric passport is a European-wide topic with major privacy concerns. The German experience presents a particularly privacy-friendly transposition for passports (no central database, no fingerprints of children under 12).

- **Interpersonal communications**

The electronic communication data retention directive and its implementation in Germany has been one of the major privacy-related topic in the past couple of years in this country. German civil society has proved to be extremely active in trying to limit the German implementation and the Constitutional Court will take into consideration how the new law fits in the German Constitutional Jurisprudence.

- **Social networks as new gate keepers of communications**

Social networks in Germany is presenting the major websites in this category visited by Germans and an overview of the activities of the Data Protection Authorities from Federal and State level, including the German activities on self-regulation of the social networks. The presentation also reveals information on the local studies on social networks in Germany and the civil society reaction to the major social networks privacy-related issues.

I.5. Conclusions

Germany has a long and powerful tradition in the field of data protection. Its Constitutional Court jurisprudence in the field, as well as the dual system (Federal – Lander) of protection of personal data has been so far a viable solution for a consistent protection of personal data, at least by comparing the system with the implementation of similar obligations in other European countries. Also, as it can be acknowledged from the latest changes in the BDSG, it has been open to adopt new institutions in the data protection field, such as the mandatory data breach notification or the company's internal data protection officer.

At the same time, Germany has a strong and very active civil society stream in the field of privacy. Its latest successes, both in terms of organisation, but also of civic involvement of a large number of people show us a best practice use of web 2.0 techniques to boost privacy activism.[29]

However we can still notice a lag between the Federal Constitutional Court Decisions and its implementation in all landers, if we look at the case of car number plates decision, where in one

29 See presentation Privacy Activism 2.0 lessons learned from the fight against data retention in Germany by Ralf Bendrath from www.vorratsdatenspeicherung.de and bendrath.blogspot.com made at CFP 2009 available at http://www.slideshare.net/cfp2009/ralf-bendrath-privacy-activism-20

year after the decision there were still 4-5 lander whose legislation does not offer enough protection according to the Constitutional decision.

Another interesting development in Germany that might influence the European framework is the attempt to use self-regulation in the field of local social networks, pushed in reality also by discussions of regulating this field through “hard law.” However, we must underline that there is no involvement of the DPAs, civil society or Consumer protection organizations in drafting the code or then applying it. At the same time, at this point in time, there is no public information regarding its effect on the privacy issues that come up with the social networks usage.

II. Mobility Fact Sheets

II.1. Car Plates Recognition

THEME	Mobility
Identification of technology	**Car plates Plate Recognition**
Technology used/tool (For each teams, a card pro tool)	**digital cameras and software similar to Optical Character Recognition (OCR) software to extract the registration data of vehicles**
Country/ use area	Germany – each State has a separate legislation. In March 2009 there were still 4-5 Lander that are using the system (Bavaria, Berlin, Brandenburg and Lower Saxony Mecklenburg-Vorpommern) More details on ADAC Report – see sources
Frame of use	Police
Population concerned: target and age	All vehicle owners
Trends (measured / supposed)	Number of Landers that are using the system has decreased after the German Constitutional Court Decision from 11 March 2008 when the corresponding statutory regulations in the federal states of Schleswig-Holstein and Hesse were considered unconstitutional.
Known or potentials dangers /Risks	As pointed by the German Federal Constitutional court: the mass screening of the number plates are equivalent to "complete surveillance" of broad parts of the population. The law need to provide enough restrictions on the use of license plate scanning.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	The mass screening would have checked the number plates against several databases already in police administration (such as the databases of stolen cars, toll, etc.) The Constitutional court decision considered that such a screening would be constitutional only if the data would be irrevocable deleted after it has been compared against an existent database. The court accepted only limited usage of the scanning: e.g. random sampling of license plates or mass scanning near borders.
What justifies the inscription in the file /Risks?	n/a
Purposes /contents, main data included / Risks?	Scope: targeting car thefts and their usage in committing other crimes ; paying road-related taxes.
File masters? Risks?	Suspicion of every regular citizen. System also logs automatically the place, time and direction of each car When using this technique.

Who accesses the files/ Sharing of the data base? Access limits? /Risks	Police forces in each Lander. Not clear if the data would not be shared with the intelligent services. Risk of mass movement profiling.
Data retention delays/ risks Right to be forgotten	Depends on each Lander legislation. Some Lander legislation still have provisions that do not list the right to delete the date, as the German Federal Court has decided. See ADAC report for details on each Lander
Rights to know or to modify data?	According with Data Protection Act in each lander.
Covert purposes/ Risks/uncontrolled future evolution	States not applying the German Constitutional Court Decision. Some Landers (such as Baden-Württemberg) have major procurement plans in this respect.
Others (interconnections…)	Discussions in some states to provide the data to the intelligence services
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Police Act in each Lander that has accepted this possibility. 11 Landers have a scheme in place for Plate scanning. Only 4 of them have their provision in agreement with the Court decision. See details in ADAC report Data protection acts in each lander German Federal Constitutional Court Decision from 11 March 2008
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Five Landers have announces that they will modify the Lander legislation in order the implement the Court decision. An action against the car plates mass scanning in Bavaria and a claim against the similar scheme in Lower Saxony has already been submitted. A constitutional complaint against the car plates scanning in Baden-Württemberg is in preparation
Conformity with the European right (Charter of fundamental rights, directives…)	n/a
Others	
This tools and young public or young adults	
How far are young people concerned?	Not specifically
Awareness of issues or of risks	ADAC (Allgemeine Deutsche Automobil-Club) – Germany's largest auto club has issued several warnings and positions papers on the risks. Prof. Alexander Roßnagel has issued several reports on highlighting the unconstitutionality of the several Lander provisions.
Indifference or reaction	Several people have initiated legal action in the Constitutional Court (one of them already successful)..
Awareness campaigns/ results	Included in the topics of surveillance of full surveillance by the AK Vorrat. Campaigns and public speeches by ADAC. Negative opinions by several Lander Data protection Commissioners
Good practises	The limitation of the deployment of mass car plates screening, through the

	jurisprudence of the Constitutional Court on the interpretation of the "right to self-determination".
Campaign to be led. On which themes?	Actions in court in Bavaria and Lower Saxony that could lead with other Constitutional Court decisions.
Others	
Conclusions	The decision of the German Constitutional Court have been instrumental in specifying the legal conditions, according to the German framework, in which a system on car plates screening could function. The determination of civil society actors has paid off in having a clear picture of what is allowed and what is not, according with the data protection legislation and constitutional law.
Recommendations	Comparing this file with the UK on the Automatic Number Plate Recognition
References	- German Federal Constitutional Court Decision from 11 March 2008 - BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. (1 - 185) http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html – Press release – Constitutional Court (only in German) – 11 Match 2008 - Hessische und schleswig-holsteinische Vorschriften zur automatisierten Erfassung von Kfz-Kennzeichen nichtig - http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-027.html - ADAC - Kennzeichenscanning Umsetzung der Vorgaben des Bundesverfassungsgerichts (03.2009) http://www1.adac.de/images/2009-03-Expertise-Umsetzung-des-BVerfG-Urteils-Kennzeichenscanning-Kurzfassung_tcm8-251695.pdf - ADAC - Kennzeichenscanning Autofahrer weiter unter Generalverdacht ADAC: Fünf Bundesländer setzen Verfassungsgerichtsurteil nicht um (23.04.2009) http://www1.adac.de/images/2009-04-ADAC-Presse-Kennzeichenscanning_tcm8-251694.pdf Pforzheimer Zeitung, More rights for the Police, 29.02.2008 - http://www.pz-news.de/Home/Nachrichten/Suedwest/Mehr-Rechte-fuer-die-Polizei_arid,22316_regid,1_puid,1_pageid,26.html Der Spiegel , 'The Hallmarks of a Totalitarian State', 12.03.2009 http://www.spiegel.de/international/germany/0,1518,541025,00.html – PHR2006 - Federal Republic of Germany , 18.12.2007 – http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559535#[58] – Heise, Hesse expands police powers, 15.12.2004 – http://www.heise.de/newsticker/Hessen-dehnt-Polizeibefugnisse-deutlich-aus--/meldung/54298 – **Daten-Speicherung.de - ADAC: Kfz-Massenabgleich durchweg verfassungswidrig** (12.07.2009) - http://www.daten-speicherung.de/index.php/adac-kfz-

massenabgleich-durchweg-verfassungswidrig/

Action against the Bavarian scheme: http://www.daten-speicherung.de/data/Klageschrift_Kfz-Massenscanning_By_2008-06-02_anon.pdf Klageschrift_Kfz-Massenscanning_By_2008-06-02_anon.pdf

Constitutional complaint against the niedersächsische scheme: http://www.daten-speicherung.de/data/ Klageschrift_Kfz-Massenscanning_Nds_2008-05-26_anon.pdf

– **FDP will hessische Polizei aufrüsten** – *11.07.2009*
http://www.daten-speicherung.de/index.php/fdp-will-hessische-polizei-aufruesten/

– Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention - Gerrit Hornung and Christoph Schnabel - University of Kassel, Germany, Computer Law & Security Review - Volume 25, Issue 2, 2009, Pages 115-122

– Hornmann: *Verfassungswidrigkeit der Befugnis über den automatisierten Kfz-Kennzeichenabgleich im Hessischen Polizeirecht*. In: *Neue Zeitschrift für Verwaltungsrecht* . 2007, ISSN 0721-880X, S. 669.

– Roßnagel: *Verdachtlose automatisierte Erfassung von Kfz-Kennzeichen*. In: *Deutsches Autorecht*. 2008, ISSN 0012-1231, S. 61.

–

III. Biological Identity Fact Sheets

III.1. Biometrics – ePass, the German biometric passport

THEME	Digital Identity
Identification of technology	**Biometrics**
Technology used/tool (For each teams, a card pro tool)	**ePass, the German biometric passport**
Country/ use area	Germany
Frame of use	Normal passport uses: travel and identity document
Population concerned: target and age	Nationals over 24: a 10-years passport, with biometrics Nationals under 24: a 6-years passport, with biometrics National under 12: a 6-years passport, WITHOUT biometrics
Trends (measured / supposed)	The biometric passport is an obligation in EU countries (Council Regulation (EC) No 2252/2004 of 13 December 2004). Germany was the first country to adopt biometric passport. Introduced in 2005 with digital photograph in an RFID chip, the passport also contains 2 fingerprints in its RFID chip since 2007.
Known or potentials dangers /Risks	Usual dangers related to biometric IDs and to RFID chips. No specific issue with German implementation.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	No central database (it is forbidden by law) Fingerprints are only in the ePass RFID chip. They are destroyed after their inclusion in the chip. NB. Information below in the same section are related to the RFID chip, not to database.
What justifies the inscription in the file /Risks?	Mandatory feature of the ePass since 2007.
Purposes /contents, main data included / Risks?	Purposes: Claimed purpose is higher security, fight against identity fraud,. It is also an obligation under EU regulation. Content: - biographical data (first name and family name, date of birth, sex and nationality of the document holder) - document-related data: serial number, issuing state, document type and expiry date, - (biometrics) digitized facial photograph and 2 fingerprints
File masters? Risks?	N/A
Who accesses the files/ Sharing of the	Border police when reading the RFID chip at the frontier

data base? Access limits? /Risks	
Data retention delays/ risks Right to be forgotten	The passport is valid 10 years for persons above 24 and 6 years for others.
Rights to know or to modify data?	Individuals may access the data at the passport authority: citizens can view the data stored in their ePassport chip using special display devices, the ePassport readers.
Covert purposes/ Risks/uncontrolled future evolution	Risks (related to biometrics): false positives and false negatives.
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	EU Council Regulation (EC) No 2252/2004 of 13 December 2004. ICAO technical standards for passports. German Passport Act of 1986, amendment of July 2005.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	N/A
Conformity with the European right (Charter of fundamental rights, directives…)	Not challenged.
Others	
This tools and young public or young adults	
How far are young people concerned?	Not specifically targeted. Children under 12 protected since their fingerprints are not taken.
Awareness of issues or of risks	No real awareness, besides some privacy organizations.
Indifference or reaction	Indifference and consent.
Awareness campaigns/ results	No real campaign. But the Chaos Computer Club (CCC German NGO) published in 2005 a manual on how to fake the fingerprints used in the biometric passport. The procedure involves coping a fingerprint from a glass and transferring it to a latex dummy that can be used to fool the reader during border check. CCC has made public demonstration on the tactic. Further, in April 2008, the CCC has published in the latest issue of their magazine Die Datenschleuder the fingerprint of one of the best known proponents of digital

	fingerprints in passports - Mr. Wolfgang Schäuble, the German Minister of Internal Affairs. The fingerprint has been printed on a plastic foil, that can replicate the fingerprint when it is pressed on a biometric reader. CCC activists wanted to make a point in their fight against digital fingerprints in any ID document, considering such data is easy to collect and reproduce.
Good practices	No central database, neither at federal nor at local level. No fingerprints taken for children under 12.
Campaign to be led. On which themes?	N/A
Others	
Conclusions	The EU Regulation has been an opportunity to implement or to enlarge the routine use of biometrics at national level. While this regulation is only for passports, it opened the way in many countries, as well as at the EU level, for more use of biometrics in ID documents, including national ID cards. While Germany has opted for a particularly privacy-friendly transposition for passports (no central database, no fingerprints of children under 12), this is not the case in other countries.
Recommendations	Need for strong limitations at EU level on the use of biometrics, especially with regards to children and with regards to centralized databases.
References	Wikipedia webpage on German passport (http://en.wikipedia.org/wiki/German_passport) Germany chapter, EPIC&PI PHR2006 Report (http://tinyurl.com/5lv48v) Centre for German Legal Legislation (http://www.cgerli.org/) German Federal ministry of Interior, webpage on ePass (http://www.epass.de/) Bundesdruckerei GmbH (industry provider, former federal printing office), Guide to the German ePassport System 2007 (http://tinyurl.com/m7dg7c) EDRIgram article, 'Germany: Biometric Passports In November', 14/07/05 (http://www.edri.org/edrigram/number3.14/biometrics) EDRIgram article, 'Fingerprinting The Fingerprint Proponent', 09/04/08 (http://www.edri.org/edrigram/number6.7/fingerprint-schauble)

IV. Interpersonal Communications Fact Sheets

IV.1. Communication Data retention

THEME	**Interpersonal Communications**
Identification of technology	**Data Retention**
Technology used/tool (For each teams, a card pro tool)	**Retention of Data during an electronic communication**
Country/ use area	Germany
Frame of use	Telecom operators (including Internet service providers) are required to retain communication data for 6 months on their servers, so that government agencies may access them.
Population concerned: target and age	General population, all telecom operators subscribers and users of fixed and mobile telephony, and internet services.
Trends (measured / supposed)	The trend for data retention at national level and at the EU level and mutually reinforcing and justifying each other. When the 1997 Directive was in force, telecom operators had the obligation to erase of anonymize communication data after the communication was completed. They could only keep these data for billing and network management purposes. The revision of this Directive in 2002 opened the way for governments to access these data. Further in 2006, the data retention Directive has rendered mandatory the retention of communication data for a period varying between 6 and 24 months. No data yet at German level.
Known or potentials dangers /Risks	Mass surveillance and profiling of interpersonal communications and networks.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	Telecom operators are required to retain data on their own servers, and respond to public authorities requests.
What justifies the inscription in the file /Risks?	Use of telecom or electronic communication means: fixed and mobile phones, emails, instant messaging, ...
Purposes /contents, main data included / Risks?	Purposes: Billing and network management purposes by telecom operators, plus use by public authorities, as provided by the Data Retention law Content: - Phone calls ((landline, mobile or VoIP): Date, time, length and involved numbers of all phone calls - Mobile phone calls: additionally, the location of the phone at the time of the call,

	the IMSI code of the phone and SMS connection data - Internet access: IP address, date, time and length of the connection, and the line which was used. - E-mail: e-mail-addresses involved and the header of each e-mail
File masters? Risks?	Telecom operators (including Internet Service Providers). Risks are high for the security of data, as well as for misuses of the data by commercial companies.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	- the police, courts and public prosecutors for the prosecution of crime - the police for the prevention of substantial dangers to public safety - secret services for intelligence purposes The access of this information for intelligence purposes by secret services as well as by the police for so-called 'prevention' purposes involves a high risk of profiling innocent users.
Data retention delays/ risks Right to be forgotten	6 months.
Rights to know or to modify data?	According to the Data Protection Act.
Covert purposes/ Risks/uncontrolled future evolution	Routine intelligence. Other risk is related to the increasing difficulty to differentiate between communication data and content data, especially with new and future communication services.
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Law on the reorganization of the telecommunications surveillance and other covert investigative measures, as well as to implement Directive 2006/24 / EC (Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG), of 21 December 2007.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	No revision yet.
Conformity with the European right (Charter of fundamental rights, directives…)	The conformity of the legislation is being challenged before the Constitutional Court. On 16/03/09, the Administrative Court of Wiesbaden found the blanket recording of the entire population's traffic data on telephone, mobile phone, e-mail and Internet usage is disproportionate. The decision of the court is "that data retention violates the fundamental right to privacy. It is not necessary in a democratic society. The individual does not provoke the interference but can be intimidated by the risks of abuse and the feeling of being under surveillance (...) The directive (on data retention) does not respect the principle of proportionality guaranteed in Article 8 ECHR, which is why it is invalid."
Others	

This tools and young public or young adults	
How far are young people concerned?	Not specifically targeted, but they are concerned to a large extent since electronic communications and instant messaging systems are their preferred modes of communication.
Awareness of issues or of risks	Very high level of awareness.
Indifference or reaction	Class action complaint filed by 34000 persons before the Constitutional Court against the data retention law. Massive protest campaigns and demonstration against data retention law, and in favour of privacy and freedoms: the 'Freedom not Fear!' demonstration gathered thousands of people in Berlin on October 2008.
Awareness campaigns/ results	Main campaign led by AK Vorrat (German Working Group on Data Retention), a German wide coalition of civil rights campaigners, data protection activists, human rights organizations, and Internet users. The campaign has met a big success since it started. It initiated the class action constitutional complaints and prepared the demonstrations.
Good practices	None
Campaign to be led. On which themes?	Already in place.
Others	
Conclusions	The EU Data retention Directive has been an opportunity to implement or to enlarge data retention at national level.
Recommendations	Campaign at EU level against Data retention Directive.
References	German federal Data protection Authority website (http://www.bfdi.bund.de) AK Vorrat, German Working Group on Data Retention (http://www.vorratsdatenspeicherung.de/) EDRIgram articles on data retention in Germany (http://www.edri.org/edrigram)

V. Social Networks Usages

V.1. Social networks websites used in the Germany

Germany is one of the European countries with the most Internet users, with an estimated number of 37.6 million visitors in January 2009.[30] As expected, one of the fastest growing website categories is the social networking. The number of Germany visitors to social networking websites was around 23.6 million, and it has increased with 11% with the same period of the last year.

As regards the most popular websites, German users seem to prefer a mostly local brands, with a second place for the worldwide targeted social networking websites that have launched localized versions of their networks. But even local brands are generally targeting more than Germany and extend to the German-speaking population, especially in Austria and Switzerland. A more detailed study by Comscore[31] on social networking websites in Germany with the data from July 2007 underlines the trend mentioned above:

A Selection of Leading Social Networking Sites Ranked by German Unique Visitors* July 2007 Total German, Age 15+ – Home and Work Locations** Source: comScore World Metrix	
Property	Total Unique Visitors (000)
Total German Internet Audience	32,924
Social Networking	14,804
MYSPACE.COM	3,650
StudiVZ Sites	3,113
JUX.DE	2,614
PICZO.COM	2,004
STAYFRIENDS.DE	1,335
NETLOG.COM	1,251
SEVENLOAD.COM	1,143
Xing	685
Skyrock Network	507
MSN Groups	440

30 Data made public by Comscore on 9.03.2009, study made on total German users, Age 15+ - Home and Work Locations - Social Networking and Multimedia among Fastest Growing Online Categories in Germany during Past Year available at http://www.comscore.com/Press_Events/Press_Releases/2009/3/Fastest_Growing_German_Websites

31 Study made available by Comscore on 18.09.2007 - study made on total German users, Age 15+ - Home and Work Locations - German Social Networking Community Reaches 14.8 Million - available at http://www.comscore.com/Press_Events/Press_Releases/2007/node_1285/Social_Networking_Sites_in_Germany/(language)/eng-US

The more recent study by Comscore[32] also showed a big increase in the usage of 2 new social networking websites: Yasni.de and Facebook.com comparing with the data from January 2008.

We need also to consider for Germany the ranking based on the number of visits/month made public by IVW (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern)[33]. We will compare recent data[34] with the data from September 2008 as provided by Christian Fuchs[35];

Name of the website	Number of visits 09.2008	Place in top IVW 09.2008	Number of visits 07.2009	Place in top IVW 07.2009
studiVZ	158.5	4	177.2	4
schülerVZ	134.4	5	154.2	6
Wer-kennt-wen	112.3	6	157.4	5
MySpace	49.6	14	53.9	13
meinVZ	45.58	16	99.2	10
Lokalisten	30.6	19	42.6	20
StayFriends	16.7	32	24.3	26

The number of opened accounts from Germany is not public, but estimates[36] regarding the number of accounts by the German major Social networking brands are that StudiVz networks (including schulerVZ and MeinVZ) has 13 million users , Wer-kennt-wen – 6.5 million and Lokalisten – 3 million registered users.

V.2. Information Commissioner and social networking

The Federal Information Commissioner and the Regional (Lander) Data protection commissioners are active in informing the public about the Internet usage and its potential dangers for privacy. One of the specific chapters is the social networks and its usage, especially by teenagers.

The Commissioners gather together in the Düsseldorfer Kreis, which is an informal association of the major Data protection regulators in Germany, that deals with the application of the data protection principles in the non-public area. In their meeting on 13 April 2008, they have issued a

32 Op cit, see 1.

33 Centre for Circulation Analysis – the German body that provides the circulation figures for advertising media Information publicly available at http://www.ivw.eu

34 Data for number of visits for July 2009 as available on ivw.eu

35 Social Networking Sites and the Surveillance Society - A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance
Christian Fuchs - Salzburg/Vienna

36 Estimates by Der Spiegel for June-July 2009 – See article Warnings against social networks (only in German, 17.07.2009) – online at http://www.spiegel.de/netzwelt/web/0,1518,636092,00.html

common decision[37] in relation with the social networks and their processing of personal data. They have made a public call for the German providers to respect the data protection framework and reminded the applicable legal provisions.

Special sections or guides on how to use the social networks and keep the privacy have been developed by several Lander Data Protection Authorities (DPA)[38] Other Lander DPAs, such as the one in Saar Lander,[39] have launched specific websites with information on data protection,[40] which present the privacy-enhancing features on the most important German social networks.

The Schleswig-Holstein DPA has been involved in European projects on privacy, that include the discussion of social networks. They are one of the partners of the European Privacy Open Space thematic network for privacy infrastructures. The DPA is also involved in the consortium of the Prime Life[41] project, which is a research project aimed to bring sustainable privacy and identity management to future networks and services. The first seminar took place with the theme Workshop on the Future of Social Networking in January 2009.[42]

The Berlin Commissioner for Data Protection has been very active locally and internationally in the theme of social network. He was the initiator of a Proposal for Resolution on Privacy Protection in Social Network Services[43], which was adopted by other Data authorities from around the world at the 30th International Conference of Data Protection and Privacy Commissioners that took place in Strasbourg, 17 October 2008, which stressed the that „it is necessary, in the first place, to carry out an in-depth information campaign involving all public and private stakeholders in order to prevent the multifarious risks associated with the use of social network services."

The Commissioner DPAs have been active in criticizing the local social networks, when their practices have raised problems with its users. The social networks could be also subject to special regulation, as proposed[44] by the Green Party in February 2009, when they considered that the German Federal Data Protection Act could be amended, in order to foresee a quality seal for social networks, but also to limit the possibilities to share the data gathered with third parties.

---

37 Text of the decision only in German at http://www.bfdi.bund.de/cln_118/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke.html?nn=409242

38 See for example the Berlin DPA - http://www.datenschutz-berlin.de/content/themen-a-z/internet/soziale-netzwerke-und-datenschutz, the Rheinland-Pfalz DPA - http://www.datenschutz.rlp.de/downloads/oh/oh-Selbst_DS_soziale_Netze.pdf or NiederSachsen - http://www.lfd.niedersachsen.de/master/C54257318_N54257107_L20_D0_I560.html

39 http://www.lfdi.saarland.de/

40 See the website at www.datenparty.de

41 For more infor about the Prime life project, see http://www.primelife.eu/

42 The report on the seminar and the presentations are available http://www.w3.org/2008/09/msnws/

43 Adopted text of th resolution available at http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

44 See Greens want BDSG-novella , 24.02.2009 – only in German http://www.datenschutz.de/news/detail/?nid=3407

Probably also as an answer to these allegations, the major German social networking websites (StudiVZ, SchülerVZ, MeinVZ, Lokalisten and wer-kennt-wen.de) have adopted on 11.03.2009 a voluntary code of conduct[45] on child, consumer and data protection issues.
The code of conduct includes the obligation to provide an easy accessible button to delete a user profile completely. This deletion needs to include all uploaded content. Comments in forums might be made pseudonymous. Another important provision is that default settings should not allow profiles of children under 14 to be visible to other people besides their connections. The profiles of all users under 16 should be restricted to be accessible by search engines.
The Code was seen by the Deputy Data Protection Commissioner of Berlin, Thomas Petri, as a step forward within the limits of the legislation, but he also questioned if the collection sensitive data by the social networks sites met the legal requirements.

V.3. Local reactions (campaign, cases, etc.)

A detailed study[46] performed by Christian Fuchs shows that the Terms of Use of the StudiVZ platform, which is popular among German speaking Internet users, is more read. This is explained by the change of its Terms of Use in December 2007, when it was introduced a new provision that
that personalized advertisements are possible. With the new terms, the users can opt out of personalized ads, but the standard option is to receive them.
The Study points out that "media information and an online information campaign seem to be some of the causes of the high degree of knowledge and the high degree of critical information behaviour of the students in our sample in respect to studiVZ."

Thus it underlines the coverage in the German press of the change of the terms of use. In December 2008, Bild Zeitung presented ten digital flops of the year 2007. studiVZ was listed at rank number 4, arguing that studiVZ has introduced "new dubious terms of use", based on which "user data will be assessed and used for personalized advertisement and ads per email and mobile phone. Furthermore data shall be passed on to public authorities"
But besides news coverage on the new studiVZ terms of use, there was also an online campaign, which was likely to attract many studiVZ users. On December 7, 2008, there were 248 interest and discussion groups on studiVZ that covered the issue of the new terms of use.
Other complaints on the way StudyVZ conducts its businesses are also present[47] in various blogs and forums.

Another German-focused study[48] made at the Fraunhofer Institute for Secure Information Technology SIT from September 2009 concluding that the social networks threaten privacy, after a series of tests made on Facebook, studiVZ, MySpace who-knows-whom, lokalisten and business-oriented portals XING and LinkedIn. The scope of the study was to to provide an initial framework for assessing the privacy protection of social networks platforms set up. The study was based on a tester, that used the networks as a regular user, but also showed the role of an

45 Text available at http://www.fsm.de/inhalt.doc/VK_Social_Networks.pdf (only in German)
46 Op cit, see 6
47 See a summary of the major complaints against the site on http://www.karsten-wenzlaff.de/2006/11/20/studivz-encyclopedia-the-most-complete-summary-until-now/
48 The report is available only in German at http://www.sit.fraunhofer.de/fhg/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf

attacker trying to get personal information about the normal user. The study includes information on how to protect the personal data in the various platforms in the best possible way.

Federation of German Consumer Organisations (VZBV)[49] has been on the top of the most important actions in Germany from the consumers side against the social networks for their breach of privacy. It started in 2008, when, after the much-debated change of the Terms of Use of StudiVZ, the organization publicly protested with the company asking to respect privacy of its users. Since StudiVZ did not comply with all the demands, VZBV started a legal action[50] against the most important German social network company.
The case is still pending, but some of the demands of the VZBV have been implemented, after the adoption of the Code of Conduct by German social networks and the public presentation of a "manifesto"[51] to ensure its users' property over their personal data.

But the VZBV did not stop here and has sent in July 2009 a series of letter of cease and desist to other social networks platform in Germany :Facebook, Lokalisten, MySpace, Wer-kennt-wen and Xing. They asked the change of the terms of use, so to be sure that the subscribers data is being used only if they consent to it – and they should decide if the search engines can see their data or not. The press release of the VZBV [52]said that in the current status the consumer is the Poor and social networks take advantage of this position. VZBV also announced they would start legal actions against the companies present on the German market, if they do not accept clarify their position. One of the targeted companies – Xing – was quick to reply[53] that it will change its terms of use in order to comply with the demands.

---

49 Http://www.vzbv.de/start/index.php?page=english

50 More infor in German, 18.02.2008 - http://www.heise.de/newsticker/Verbraucherschuetzer-feuern-juristisch-gegen-StudiVZ--/meldung/103458

51 More info at StudiVZ gibt Datenschutzversprechen - http://www.heise.de/newsticker/StudiVZ-gibt-Datenschutzversprechen--/meldung/142660

See the Manifesto (only in German) at http://blog.studivz.net/2009/07/28/vz-gruppe-startet-datenschutz-kampagne-%E2%80%9Edeine-daten-gehoren-dir%E2%80%9C-und-gibt-mitgliedern-ein-umfassendes-sicherheitsversprechen/

52 See Facebook sued over privacy - 14.07.2009 http://www.news24.com/Content/SciTech/News/1132/7cd9d35d9d55494a93005b5b318c366a/14-07-2009%2009-07/Facebook_sued_over_privacy

53 According to Heise – article in German 15.07.2009 - http://www.heise.de/newsticker/Xing-folgt-Forderungen-von-Verbraucherschuetzern--/meldung/142060