European Court of Human Rights
Council of Europe
F-67075 Strasbourg cedex

Application no. 50001/12

Breyer v. Germany

28/10/16

A. Domestic law and practise

1. The government's report on the domestic law is correct but incomplete.
2. In addition to subscriber data, telecommunications providers store traffic data pertaining to the location of mobile devices as well as to the details of any communication.
3. According to § 96 and § 97 of the Telecommunications act (TKG) traffic data may be stored i.e. for billing purposes. Guidelines published by the Data Protection Commissioner[1] state that providers of prepaid services may store traffic data for a period of three months in case a customer objects to the billing of his communications.
4. According to § 100 TKG traffic data may be stored in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. According to the guidelines, all traffic data – even

[1] https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile

where not needed for billing purposes – may be stored for this purpose for seven days.

5. §§ 113a pp. even require providers to store and retain traffic data for several weeks, just in case government agencies request access (blanket data retention). The act introducing a storage obligation and a maximum retention period for traffic data came into force on 18/12/2015. The said provisions read:

§ 113a Obligated parties; compensation

(1) The obligations concerning traffic data storage, data usage and data security in accordance with §§ 113b to 113g relate to providers of publicly available telecommunications services. Any party which provides publicly available telecommunications services but does not itself generate or process all the data to be stored in accordance with §§ 113b to 113g must

1. ensure that the data not generated or processed by the party in the course of providing it service is stored in accordance with § 113b(1) and

2. inform the Federal Network Agency immediately, at its request, regarding who is storing this data.

(2) As regards the unavoidable expenditure incurred by the obligated parties as a result of implementing the stipulations arising from §§ 113b and 113d to 113g, reasonable compensation must be paid if this appears necessary in order to prevent or offset undue hardship. The costs that have actually arisen are decisive in terms of calculating the level of compensation. The Federal Network Agency shall make decisions regarding applications for compensation.

§ 113b Obligations regarding the storage of traffic data

(1) The parties mentioned in § 113a(1) are obliged to store data in Germany as follows:

1. Data in accordance with paragraphs 2 and 3, for 10 weeks,

2. location data in accordance with paragraph 4, for 4 weeks.

(2) The providers of publicly available telecommunications services shall store

1. the call number or another identifier of the calling and called line, as well as of every additional participating line in the case of call redirection or forwarding,

2. the date and time of the start and end of the call, stating the underlying time zone,

3. information regarding the service used, where various services can be utilised in the context of the telephony service,

4. in the case of mobile telephony services, also

a) the international prefix of mobile subscribers for the calling and called number,

b) the international prefix of the calling and the called terminal equipment,

c) the date and time of the initial activation of the service, stating the underlying time zone, if services have been paid for in advance,

5. in the case of telephony services over the Internet, also the IP addresses of the calling and called number and assigned user IDs.

Sentence 1 shall apply accordingly

1. in connection with the transmission of a short, multimedia or similar message. In this regard, the time the message is sent and received shall supersede the information pursuant to sentence 1 point 2;

2. to unanswered calls or those which have been unsuccessful on account of a network management intrusion if the provider of publicly available telecommunications services stores or logs the traffic data mentioned in sentence 1 for the purposes referred to in § 96(1) sentence 2.

(3) The providers of publicly available Internet access services shall store

1. the IP address assigned to the subscriber for using the internet,

2. an unambiguous call identifier via which internet access is achieved, as well as an assigned user ID,

3. the date and time of the start and end of internet usage under the assigned IP address, stating the underlying time zone.

(4) Where mobile telephony services are used, the radio cell designations which have been used by the calling and called number at the start of the call must be stored. As regards publicly available internet access services, in the case of mobile usage, the designation of the radio cell used at the start of the internet connection must be stored. In addition, data must be retained from which follows the geographical location and the main beam directions of the antennas supplying the respective radio cell.

(5) The content of the communication, data pertaining to websites visited and data from electronic mail services may not be stored on the basis of this regulation.

(6) Data underlying the connections mentioned in § 99(2) may not be stored on the basis of this regulation. This shall apply, mutatis mutandis, to telephone connections emanating from the authorities mentioned in § 99(2). § 99(2) sentences 2 to 7 shall apply accordingly.

(7) The data shall be stored so as to enable information requests from the approved authorities to be answered immediately.

(8) The party obligated in accordance with § 113a(1) must delete forthwith the data stored on the basis of paragraph 1, but at the latest within 1 week of the lapsing of the retention periods under paragraph 1, such that this deletion cannot be reversed, or must ensure irreversible deletion.

§ 113c

Data usage

(1) The data stored on the basis of § 113b may

1. be transmitted to a criminal prosecution authority if this authority demands transmission by invoking a provision of the law which allows it to collect the data referred to in § 113b for the purpose of prosecuting particularly serious criminal offences;

2. be transmitted to a public risk prevention authority in the Federal States if this authority demands transmission by invoking a provision of the law which allows it to collect the data referred to in § 113b for the purpose of averting specific risks of a person being killed, injured or deprived of their freedom, or specific risks relating to Federal Government or Federal State holdings;

3. be used by the provider of publicly available telecommunications services for information purposes according to § 113(1) sentence 3.

(2) The data stored on the basis of § 113b by the parties obligated in accordance with § 113a(1) may not be used for purposes other than those stated in paragraph 1.

(3) The data are transmitted in accordance with the statutory instrument pursuant to § 110(2) and the Technical Guideline as per § 110(3). The data must be identified in such a way that it can be discerned that it constitutes data which was stored in accordance with § 113b. Once the data has been transmitted to another authority, the latter must maintain this identification.

6. Since the collection of traffic data on all communications and movements cannot be evaded, the only chance of using electronic communications without easily being identifiable is in not identifying yourself when subscribing to the service. This window for anonymous communications, which even the infamous EU Data Retention Directive kept open, is closed by the contested provision of § 111 TKG which makes identification mandatory.
7. As to the domestic practise it should be noted that the numbers of automated accesses to subscriber data (§ 112 TKG) has risen from 26.62 million in 2008 to 34.83 million in 2015.[2]

[2] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2016/Jahresbericht2015.pdf?__blob=publicationFile&v=2

8. The number of court orders to disclose traffic data for law enforcement purposes has climbed from 13.426 in 2008 to 26.265 in 2015.[3]

B. The law

I. First question asked by the Court (alleged violation of Art. 8 par. 1 ECHR)

9. The government disputes that Art. 8 par. 1 ECHR encompasses a right to communicate anonymously, but concedes that § 111 TKG interferes with the human rights enshrined in Art. 8 par. 1 ECHR.

10. The application explains in detail why Art. 8 par. 1 ECHR encompasses a right to communicate anonymously. The interveners have added more arguments. There is no need to repeat all of what has been written. If the right to privacy means that every individual may decide on whether to disclose personal data or not, that evidently means that every individual may decide not to disclose their identity and remain anonymous when communication.

11. The government claims that the applicants seek generally anonymous communications and a ban on government agencies to identify communications even where needed for law enforcement or averting danger, setting the interest in anonymity absolute and making legitimate requests impossible.

12. This claim is false. In truth it is the government that seeks a general ban of anonymous communications even where a subscriber is not even remotely connected to a crime or danger. The government is setting the interest in identifiability absolute and makes legitimate anonymity impossible. It does not balance the rights and interests concerned but seeks absolute identifiability and traceability of electronic communications and movements with telecommunications devices.

[3] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html;jsessionid=DE784B7E4415E-B2A83184DA19F93D009.1_cid377

13. Removing § 111 TKG is the only way to establish a proper balance between the right to privacy and correspondence and the public interest in law enforcement and security. In general subscribers may communicate anonymously using prepaid SIM cards (contractual subscribers will be identifiable anyway). But when there is a legitimate interest in the identity of a subscriber, the competent agencies may use ample means to identify them, including data on the sale and recharges of the SIM card, traffic data on whom the subscriber communicates with and location data on the subscribers whereabouts. These means of identification are much more reliable and not as easy to circumvent as subscriber data.

14. The application explains in detail which other means of identification are available to the government and are being used successfully in many other countries that do not force every subscriber to identify without cause. We cited a government official who considered unregisters prepaid SIM cards a useful tool to lure criminals into believing that they are untraceable. Again I would like to cite an internal EU document[4] dating back to 2000:

FI, PL, and SE stated "there is no interest" in obliging users to register their identities. SI, RO, IE, DK, PL, CZ. and UK reiterated that they were not in favour of imposing an obligation of users of pre-paid SIM cards to register them. Apart from opportunity crime that could be triggered by this registration, police avails of other techniques to establish the ID of anonymous users. It would also lead to public resentment. Besides, it would be easy to bypass any obligation which would annul the positive effect of that legislation. Some conceded that the only useful level of regulation would be at EU level.

[4] http://wiki.vorratsdatenspeicherung.de/images/2010.05.04_report_meeting_w_MS_12_March_2010.pdf

15. The government disputes that subscriber data can be used to monitor everyday communications and movements, and stresses the differences between subscriber and traffic data.

16. However the application at length explains that information establishing the identity of the user of electronic communications devices is an integral part of all communications made using this device. Both subscriber data and traffic or content data are usually not very meaningful by themselves, but extremely sensitive in combination. The applicants maintain that subscriber data, in combination with other data, can be used to monitor a person's everyday communications and movements. Knowing the identity of a subscriber is the key to exploiting the wealth of information contained in communications data and patterns.

17. The government disputes that § 111 TKG amounts to a ban on anonymous communications, referring to internet cafés and Internet communications services.

18. It is true that savy users and professional criminals can still find ways of communicating anonymously, for example using prepaid cards registered by another person (e.g. a homeless person who would like to earn some money) or prepaid cards from a country that does not require identification (the EU is to cut roaming rates in the EU which makes this an attractive option, making § 111 TKG easy to circumvent despite the new obligation to show an ID). For the average person and the average communication, however, these means are too tedious and complicated to use. § 111 TKG prevents the general population from communication anonymously.

19. As to Internet communications services (e.g. Whatsapp or Skype), they cannot replace telephone calls in most circumstances. In addition, their providers generally collect users' IP addresses which in turn can be traced to the Internet subscriber because of § 111 TKG.

20. The application deals with this issue in more details and shall not be reiterated.

21. The government claims that § 111 TKG is a suitable instrument to improve law enforcement and maintenance of order. Although subscriber data may be useful for those purposes occasionaly, the application explains that there are other and less intrusive ways of identifying users, and that a blanket identification requirement does not increase the crime clearance rate in sum. There is no need to repeat these arguments in detail.

22. The government disputes that § 111 TKG makes information available to authorities that are more sensitive than DNA data and fingerprints. The applicants maintain their position, referring to the arguments set out in the application.

23. The government claims that a general obligation to identify avoids stigmatising people suspected of a crime. However, the negative consequences of stigmatisation cannot be averted by simply interfering with all citizens' human rights. Identifying the entire population is a far greater interference than identifying suspects. With regard to a similarly blanket interference, the EU Court of Justice correctly argued as follows:[5]

Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in par-

[5] Judgement in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland.

ticular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

24. The court's finding of disproportionality encompassed the provisions on subscriber data contained in Directive 2006/24. It should be stressed that Directive 2006/24 mandated the retention of data processed in the course of business, whereas § 111 TKG mandates even the collection of data that would normally not even be needed.
25. The government points out that in Marper, DNA and fingerprint data could be stored indefinitely. However, the same is the case with § 111 TKG as people generally use their telephone numbers for a lifetime.
26. Similarly to Marper, with § 111 TKG the German government established an identification and ID requirement which goes beyond what most other governments do. A diverging practise among convention states does not necessarily speak for a wide margin of discretion, but raises the question of whether extreme practises can be justified where other countries can do without similar regimes.

II. Second question asked by the Court (alleged violation of Art. 10 par. 1 ECHR)

1. The government disputes that Art. 10 par. 1 ECHR encompasses a right to divulging and receiving information anonymously. The application explains the applicants' reasoning in detail. The interveners have added more arguments. There is no need to repeat all of what has been written in that respect.
2. Also, in Delfi, the Court decided that anonymity on the Internet must be balanced against other rights and interests. This underlines that anonymity is considered a right and interest.

3. The government refers to ways of communicating anonymously via the Internet and maintains that anonymous communications should not prevail absolutely. The applicants have gone into these arguments above.

Dr. Patrick Breyer