The Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg Cedex

Application no. 50001/12

Breyer v. Germany

REQUEST FOR A REFERENCE TO THE GRAND CHAMBER

29/04/20

A. INTRODUCTION

1. This application concerns a German law effectively ***banning anonymous electronic communications and Internet access*** by mandating telecommunications operators to identify all subscribers even where identification is not needed for business purposes (pre-paid SIM cards).
2. The Chamber (First Section), in its ***judgment of 30 January 2020*** ("the Judgment"), held that:
   a) The Court was not called to decide if and to what extent Article 10 of the Convention may be considered as guaranteeing a right for users of telecommunication services to anonymity,
   b) The general and indiscriminate identification of all subscribers constituted a limited and proportionate interference with their rights under Article 8 of the Convention; the level of interference was fundamentally different from that of intercepting content or accessing traffic data.

3. The Applicants request that the case be ***referred*** to the Grand Chamber pursuant to Article 43 of the Convention on the basis that it concerns a serious question affecting the interpretation of the Convention and a serious issue of general importance which warrants consideration by the Grand Chamber. The case is appropriate for referral to the Grand Chamber to enable the Court to authoritatively state the law governing mass identification and anonymity bans in light of modern technological developments. There are 15 Council of Europe (CoE) Member States with similar anonymity bans for telecommunications in place, versus 32 that do not have such laws. The authoritative analysis of the Grand Chamber is required to develop its case law appropriately, as well as to ensure the proper protection of privacy, freedom of the press and freedom of expression across the Contracting States. It is in the interests of all people and Contracting States that the Grand Chamber authoritatively address the compatibility of bans on anonymous communications with the Convention.
4. One Member State (Austria) in 2019 even proposed an anonymity ban for ***online forums***.[1] In another Member State (Germany) a legislative body is currently considering a bill that would ban the anonymous use of social networks.[2] The issue at stake is therefore of importance for potential future cases as well.

B. RIGHT TO ANONYMOUS SPEECH (ARTICLE 10)

5. The Chamber examined the complaints solely under the right to respect for private life (Article 8 of the Convention), but did not decide if and to what extent ***Article 10 of the Convention*** guarantees a right for users of telecommunication services to anonymity. It argued that this was not the „key aspect" of the complaint because the applicants had not alleged that their communications had been subject to interception or surveillance (§ 60-63 of the judgement).
6. This decision effectively means that the right to freedom of expression, to receive and impart information and ideas without interference by public authority (Article 10 of the Convention) ***does not protect against indiscriminate bans on anonymous speech*** and general requirements for persons to identify and have their

1 „Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G)".

2 „Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes zum Zweck der Erleichterung der Identifizierbarkeit im Internet für eine effektivere Bekämpfung und Verfolgung von Hasskriminalität".

identity recorded before they can express themselves. Article 10 of the Convention would only protect against government surveillance of specific persons.

I. Serious question of interpretation

7. Whether Article 10 of the Convention only protects against government access to specific speaker identities or also against the general collection and retention of speaker identities making it easy for the government to identify speakers at a later stage is a ***serious question*** affecting the interpretation of the Convention. It concerns a new issue that has never before been decided by the Court. It may also be relevant for future cases, seeing that governments are constantly considering to expand such anonymity bans (see examples above).

8. The Court has previously acknowledged in ***Delfi*** AS v. Estonia (64569/09, § 147) the importance of anonymity, noting that it has long been a means of avoiding reprisals or unwanted attention. As such, anonymity has been found capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. Given this importance of anonymity for the free flow of ideas and information, Article 10 needs to protect against laws banning this anonymity generally and indiscriminately for electronic communications of persons who are not even remotely connected with any crime or wrongdoing.

9. The Chamber's decision not to apply an article of the Convention to the collection and retention of information, but only to government access to it, is also inconsistent with previous jurisprudence. In ***Weber and Saravia*** v. Germany (54934/00), the Court accepted that a bulk surveillance regime interfered with a journalist's freedom of expression, finding that there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone (§ 145). In the present case applicant Patrick Breyer noted in the application that he is a member of a privacy watchdog NGO and publishes confidential information, including government documents for which the NGO relies on anonymous sources. The absence of anonymous communications channels can deter sources from supplying government documents to the applicant that reveal ills and abuses, thus preventing him from alerting the public to abuses of power. The applicant further pointed out that he was a Member of Parliament (of a regional parliament at the time of filing the application, presently a Member of the European Parliament) and uses electronic communications for confidential contacts with cit-

izens and whistleblowers. The absence of anonymous communications channels can deter citizens and whistleblowers from informing the applicant about ills and abuses, thus preventing the applicant from addressing and stopping such abuse of power. In the past the applicant has relied on anonymous sources for uncovering and tackling racism and sexual harassment in a police academy as well as the suppression of exculpatory information in a criminal trial by a police officer. Similarly to the Weber case, a bulk identification regime interferes with the publisher's and the Member of Parliament's freedom of expression, creating a danger that his sources might be either disclosed or deterred from calling or providing information by telephone.

10. In Financial Times (821/03, § 63) and Becker (21272/12, § 82) the Court emphasised that a chilling effect will arise wherever ***journalists*** are seen to assist in the identification of anonymous sources. Journalists forced to use a registered telephone number to communicate with anonymous sources make it easy for investigators to identify their source once the story is published. There is a public interest in receiving information imparted through anonymous sources, and the public are also potential sources themselves (Financial Times, § 63).
11. The Chamber's reasoning with a ***lack of interception or surveillance*** of the applicants communications disregards the fact that the applicants would never know had subscriber data been accessed or communications been monitored, as there are no provisions in German law to notify access to subscriber data and far-reaching exceptions to provisions on notifying subjects of communications surveillance.
12. Therefore, contrary to the Chamber's assumption, if and to what extent ***Article 10 of the Convention*** guarantees a right for users of telecommunication services to anonymity (i.e. non-identifiability) is clearly a „key aspect" of the present complaint. The Chamber missed this key aspect and did not even mention the word "anonymity" when assessing the merits of the applications.

II. Serious issue of general importance

13. In the digital age, the existence of a right to anonymous expression is a serious issue of general importance. The Chamber's decision not to apply Article 10 of the Convention to an anonymity ban ***renders the right to freedom of expression largely ineffective***. Having to identify before being able to exchange opinions electronically combined with government ability to retrace such exchanges to an identified person has a chilling effect on freedom of expression. The mere risk of

future government identification and intervention results in self-censorship in many cases, no matter if surveillance will actually take place or not (which the speaker doesn't know at the time of speaking and can't be sure of).

14. Anonymity benefits many people engaging in the exchange of ideas and opinions. Certain ***groups of people*** will speak up only when protected by anonymity. Journalists, researchers, lawyers, civil society, human rights defenders, political activists and people from marginalised or minority communities rely on anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment, intimidation, violence, or persecution. Anonymity empowers women and members of the LGBTQ community by giving a voice to those often denied their right to be heard. When one's primary means of communication is directly linked to one's real identity, the protection offered by anonymity disappears and women, sexual minorities, and other vulnerable groups are exposed as targets of surveillance.
15. ***In repressive environments*** (as seen even in some Convention states), anonymity is just about the only protection enjoyed by whistleblowers, human rights defenders, journalists, and members of the political opposition. It also gives a safer space to the marginalised by allowing them to speak out against oppression and abuse without fear of retaliation.
16. ***People without ID*** are prevented from electronically seeking and imparting information altogether by the impugned provisions. People who lack ID are excluded from using a smartphone for formulating and sharing ideas where general and indiscriminate SIM registration laws are in place. Roughly 1 billion people around the world and an estimated 4 million people in the European Union lack a valid form of government ID and could be prevented from purchasing a SIM card as a result of mandatory identification laws.
17. While there are some ***remaining ways of communicating anonymously*** despite a ban on anonymous SIM cards (particularly for savvy users and professional criminals), these are not practical and therefore no real alternative for the average person. For example if a whistle-blower used a telephone booth to inform a journalist, the journalist would not be able to get back to them with questions. The impugned provision thus prevents the general population from communicating anonymously.

18. A right to anonymous expression is largely ineffective today if it doesn't exist on ***digital networks***. People around the world now live major parts of their lives digitally. Our use of communications technology has developed greatly in the last decade. We now use the internet to impart ideas, conduct research, expose human rights abuses, explore our sexuality, seek medical advice and treatment, correspond with lawyers, communicate with friends, colleagues and loved ones and express our political and personal views. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. To a large degree they have replaced books and private diaries.
19. The ***UN Special Rapporteur on Freedom of Expression*** in his June 2015 report on encryption and anonymity noted that "compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest". He recommends that "states should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users." He concludes that "[e]ncryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."
20. The ***Constitutional Court of the Republic of Korea*** struck down anti-anonymity laws for violating the right to freedom of expression (Decision 2010 Hun-Ma 47, 252 (consolidated) of 28 August 2012). It ruled that freedom of expression includes the freedom of anonymous expression, that is without disclosing one's identity. A general identification requirement for Internet forums was ruled a disproportionate interference with that right. The Supreme Court of the United States has consistently protected the right to anonymous expression as well.
21. All this demonstrates the fundamental importance of the applicability of the right to freedom of expression to anonymity bans.

C. INTRUSIVENESS AND PROPORTIONALITY OF THE INTERFERENCE WITH RIGHTS UNDER ARTICLE 8

22. The Chamber considered the general and indiscriminate identification of all telephone and Internet subscribers an interference with the rights under Article 8 of the Convention that was "***while not trivial, of rather limited nature***" (§ 95) and fundamentally less serious than intercepting content or accessing traffic data (§ 92). The interference was found proportionate. For this assessment the Chamber relied on the EU Court of Justice's Ministerio Fiscal judgment.

I. Serious question of interpretation

23. The intrusiveness and proportionality of bans on anonymous communications and whether subscriber identity requires less protection than traffic and content data are ***serious questions*** affecting the interpretation of the Convention. They concern new issues that have never before been decided by the Court. They may also be relevant for future cases, seeing that governments are constantly considering to expand such anonymity bans (see examples above).
24. The need for an assessment by the Grand Chamber is underlined by the ***Dissenting Opinion*** of Judge Ranzoni who assesses the intrusiveness of the interference very differently.
25. While the identity of a subscriber to a telephone number is not sensitive in itself, it serves as the ***key to (sensitive) telecommunications data*** and enables a person to be linked up to a phone number or a phone number to be connected to a person. It thus facilitates the identification of the parties to every telephone call or message exchange and the attribution of possibly sensitive information to an identifiable person. Subscriber identity data is key to monitoring a target's everyday communications and movements. With regard to Internet connections, to say it with the Benedik decision, identifying a subscriber "enable[s] the police to associate a great deal of information concerning online activity with a particular individual without his or her consent" (§ 130). Knowing the identity of a subscriber is the key to exploiting the wealth of information contained in communications data and patterns. This capability is the very purpose of the provision in question but the Chamber failed to understand and appreciate this.
26. The identity register for all telephone numbers can be used by authorities to ***look up the telephone numbers used by a target*** to be able subsequently request ac-

cess to traffic data that reveals the target's contacts and movements (location), or to intercept the content of their communications.

27. Vice-versa where authorities hold intercepted content or traffic data (for example after requesting a list of telephones used in the surroundings of a suspected crime or a list of numbers dialled by a suspected offender) or a list of calls stored on a mobile phone, an identity register will allow them to ***determine the identity of the parties to specific communications***.

28. The Chamber's assessment of the level of interference is inconsistent with previous jurisprudence. In ***Benedik*** (62357/14) the Court emphasised the significance of the particular context in which subscriber identity information is used and held (§ 109): *"... Therefore what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data .... To hold otherwise would be to deny the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle."*

29. It is not possible to limit consideration exclusively to the nature of the collected and stored information. The ***usefulness and possible uses of the information*** are of decisive importance. These depend on the possibilities for processing and collating information inherent in information technology. Data that are in and of themselves of no significance can become important in another context. In that respect, as the German Constitutional Court famously held in 1983, „unimportant" personal data no longer exist in the context of automated data processing. The extent to which information is sensitive cannot depend exclusively upon whether it concerns intimate matters. Knowledge of the context in which data are used is necessary to establish the level of interference.

30. While subscriber identity data in itself is usually not sensitive, the same goes for communications data of an unidentified individual as well as the content of a conversation the participants of which are unknown. "[T]the content of communication alone [does] not have any particular weight in the absence of identification of those communicating" (Benedik, 62357/14, § 31). Any of these data are not usually sensitive in themselves, but information on the communications of an identified individual are very much so. Information establishing the identity of the user of a

telephone number is an ***integral part of all communications*** made using this number. In the context of a subscriber's communications, their identity "must … be treated as inextricably connected to the relevant ... content revealing data" (Benedik, § 109). The identity register for all telephone numbers under consideration thus does not only hold information on subscriptions, but also contains identity information on all communications made using the subscription. Thus the identity of a subscriber may "in fact [communicate] (to put it simply) traffic data in an electronic communications network regarding this person" (Benedik, § 34).

31. Assessing the general and indiscriminate identification of all telephone numbers without understanding that this removes the ***protection of confidential communications*** undermines the effectiveness of the rights under Article 8 in the digital age.

32. Taking into account the wealth of communications data accessible to authorities once the user of a telephone number is identified, subscriber identity data is more sensitive even than DNA data and fingerprints the retention of which for identification purposes the Court considered in ***Marper*** (30562/04 and 30566/04): DNA data and fingerprints cannot normally be used to gain comprehensive insight in the private life, communications and movements of a person but subscriber identity data can. In this way the Chamber's present decision deviates from the Marper judgement which found that "the blanket and indiscriminate nature of the powers of retention ... of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard". While in Marper, DNA and fingerprint data could be stored indefinitely, the same is the case here as people generally use their telephone numbers for a lifetime. Similarly to Marper, the German government established a blanket identification 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 interferences.

33. When ***comparing the intrusiveness*** of a ban on anonymous communications with accessing traffic or intercepting content, one needs to take into account the fact that access to communications takes place only on a case-by-case basis to in-

vestigate suspects, whereas the impugned law generally and indiscriminately bans anonymous communications even for persons not even remotely connected with a crime or danger. A law that interferes with the rights of the entire population is, by its very nature, extremely intrusive.

34. The Chamber's judgement is inconsistent with the Benedik judgement also regarding the conditions for ***data access***: According to Benedik it is "manifestly inappropriate" for a government authority to establish the identity of a communicating individual without a court order (§ 129). In the present case, although the impugned law does not require a court order for accessing the register to establish the identity of a communicating individual, the Chamber accepted that.

35. The Chamber relied on the CJEU ***Ministerio Fiscal*** decision (C-207/16) and its conclusion "that the access to data at issue could not be defined as a serious interference". However, a completely different issue was at stake in that case. The CJEU accepted the interference as justified "in the circumstances" of its case. That case concerned the SIM cards of one stolen mobile telephone that was linked during a period of 12 days with the identity of owners of those SIM cards. The request sought access only to the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards. Only in these circumstances the Luxembourg Court held that access to that specific data could not be defined as "serious" interference. The CJEU emphasized: "*Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period*" (§ 60). The present case is different. First, it does not concern access to data, but rather the collection and storage of data. Secondly, it does not relate to a specific criminal investigation with concrete investigative measures to be examined, but concerns an indiscriminate and general collection of data on non-suspects. Thirdly, it is – in contrast to Ministerio Fiscal – neither about very specific data (SIM cards from one telephone) nor a limited duration (12 days), but rather about the data sets of millions of people stored for a much longer period. Fourthly, the identity register for all telephone numbers makes it possible and is commonly used to subsequently ascertain the date, time, duration, recipients and even con-

tent of the communications made by a subscriber, and the locations where those communications took place.

36. In its landmark ***Digital Rights*** decision (C-293/12 and C-594/12) the CJEU invalidated the EU's Data Retention Directive not only where it mandated the general and indiscriminate retention of traffic and location data, but also the provisions that mandated the general and indiscriminate retention of subscriber identity data ("name and address of the subscriber or registered user", Article 5 of the Directive). "*Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means*", the Court reasoned (§ 26). It ruled the interference disproportionate both in regard to subscriber and traffic data because the Directive did not require any relationship between the data whose retention it provided for and a threat to public security and, in particular, it was not restricted to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved in a serious crime, or to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences (§ 59). If the CJEU considers it disproportionate to enable the government to establish the identity of any party to an electronic communication, the Chamber's decision to the contrary should not be allowed to stand unscrutinised by the Grand Chamber.

II. Serious issue of general importance

37. The impugned German law indeed ***goes beyond blanket data retention*** in one important aspect: Unlike the EU's Data Retention Directive the law does not only mandate the ongoing retention of electronic data stored for business purposes (blanket retention), but it mandates the collection of extra data the operator does not normally need and have (blanket collection), namely the identity of prepaid SIM card users. The threat blanket collection policies pose to the right to privacy is even greater than for blanket retention policies. Even the invalidated EU Data Retention Directive did not mandate identifying the subscribers of all telephone numbers, but allowed for the continued use of anonymous prepaid SIM cards.

38. The Court stressed in Delfi that the ***interest in anonymity is not absolute***. It must yield "on occasion" (§ 149) – thus not generally and indiscriminately – to other legitimate imperatives. This is ensured in the absence of an identity register for all telephone numbers: In general, subscribers may communicate anonymously using

prepaid SIM cards (contractual subscribers will be identifiable anyway). But when there is a legitimate interest in knowing the identity of a subscriber, the competent authorities may use ample means to identify them, including data on the sale and recharges of the SIM card, traffic data on who the subscriber communicates with and location data on the subscriber's whereabouts and information on the phone used (IMEI code). This data is usually sufficient to identify suspects of serious crime.

39. The proportionality of general and indiscriminate anonymity bans is a serious issue of ***general importance*** also in view of future applications of this precedent. If governments can make identification a precondition to communicating electronically, what would prevent them from making it a precondition to private life in other respects? What would prevent governments from requiring all persons entering public or private buildings or public transport to register by name? What would prevent governments from requiring citizens to visibly wear name tags in public at all times, or from deploying pervasive biometric identification systems (facial surveillance) to identify all citizens in public spaces as seen in autocratic states? Can lives be private in the meaning of Article 8 (1) of the Convention in the absence of anonymity?

40. With the impugned law the Contracting State seeks a general ban of anonymous communications even where a subscriber is in no way connected to a crime or danger. The State seeks to set the ***interest in identifiability absolute*** and makes legitimate anonymity impossible. It does not seek a fair balance of the rights and interests concerned but aims at absolute identifiability and traceability of electronic communications and movements with telecommunications devices. The Grand Chamber should consider the serious implications of such policies on democratic societies. Excessive state surveillance puts at risk the very core values protected by the Convention.

IV. CONCLUSION

41. For all these reasons, this is an exceptional case within the meaning of Article 43 and a referral to the Grand Chamber is justified.

Dr. Patrick Breyer, [...]