BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 7 • N° 28 • SEPTEMBER 2021

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

ADDING AND REMOVING ELEMENTS OF THE PROPORTIONALITY AND NECESSITY TEST TO ACHIEVE DESIRED OUTCOMES. BREYER AND THE NECESSITY TO END ANONYMITY OF CELL PHONE USERS

by Paul De Hert* and Georgios Bouchagiar**

Case of Breyer v Germany Application no 50001/12 (ECtHR, 30 January 2020)

The Breyer judgment concerns the storage of subscriber data by telecommunications service providers. To the Court, the collection and storage of such data amounted to interference of a rather limited nature. Additional safeguards were provided in the relevant German laws and there was independent supervision by the data protection authorities. The German lawmaker had not exceeded the margin of appreciation. There had been no violation of Article 8 of the European Convention on Human Rights.

Key Words: Breyer, subscriber data, telecommunications service providers, right to privacy

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
This working paper is a longer version of a published article. Please refer to the original publication as: Paul De Hert, Georgios Bouchagiar, 'Adding and removing elements of the proportionality and necessity test to achieve desired outcomes. Breyer and the necessity to end anonymity of cell phone users' European Data Protection Law Review, Volume 7 (2021), Issue 2, Pages 304 - 318.

Disclaimer

1. The Judgement: German laws ending anonymity of users of pre-paid mobile telephone SIM cards

In 2004, section 111 of the German Telecommunications Act (hereinafter: "section 111") extended existing obligations of telecommunications service providers to collect and store personal data of subscribers: from now on this obligation also included data about users of pre-paid mobile telephone SIM cards.[1] This Section 111 should be read in conjunction with sections 112 and 113 of the German Telecommunications Act (hereinafter: "section 112" and "section 113" respectively) that organise information requests by law enforcement authorities. These provisions impose duties on service providers to make available data stored via an automated procedure (section 112) or via a manual (on demand) procedure (section 113).[2]

Under section 112, the authorities, exhaustively listed therein, are entitled to access section 111-data stored via an automated and centralised procedure: data stored are made readily available by the service providers and can then be retrieved by the Federal Network Agency without the knowledge of these providers.[3]

Section 113 grants authorities (not exhaustively enlisted) the power to access data stored through a manual procedure demanding a written request.[4]

In 2005 and in the face of such storage of and access to their subscriber data, Mr Patrick Breyer, a "digital freedom fighter" with an active political profile,[5] and Mr Jonas Breyer (the "applicants") brought legal proceedings before the Federal Constitutional Court. Among others, they challenged sections 111, 112 and 113 claiming violation of their right to privacy of correspondence, post and telecommunications and their right to informational self-determination.[6]

---

* Professor, Law Science Technology & Society, Vrije Universiteit Brussel, paul.de.hert@vub.be; Associate Professor, Tilburg Law School, Department of Law, Technology, Markets, and Society, paul.de.hert@tilburguniversity.edu.

** Doctoral Researcher in Criminal Law and Technology, Faculty of Law, Economics and Finance, University of Luxembourg, georgios.bouchagiar@uni.lu; supported by the Luxembourg National Research Fund (FNR) (PRIDE17/12251371).

1 ***Breyer v Germany*** Application no 50001/12 (ECtHR, 30 January 2020) (***Breyer***), para 27 and accompanying text of section 111 of the Telecommunications Act (see ANNEX). Concerning section 111, and in addition to the duties of collection and storage regarding the case of SIM-cards, the 2004 amendments imposed an obligation on service providers to collect and store information beyond the contractual relationship (***Breyer***, paras 6-7). Furthermore, under the 2007 amendments, more data, such as the device number, were covered by the service providers' duty to collect and store information (***Breyer***, para 10). Finally, to address the ever-growing (then) phenomenon of registration of false data, the 2016 amendments to section 111 introduced the duty of the subscribers to prove their identity (***Breyer***, para 28).

2 ***Breyer***, para 27.

3 ***Breyer***, para 29 and accompanying text of section 112 of the Telecommunications Act (see ANNEX).

4 ***Breyer***, para 31 and accompanying text of section 113 of the Telecommunications Act (see ANNEX).

5 Mr Patrick Breyer is now a member of the European Parliament. In 2005, he was a judge in Schleswig-Holstein. Mr Breyer had also brought his case before the Court of Justice of the European Union (CJEU) requesting a preliminary ruling on Article 7(f) of the Directive 95/46/EC (of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31) in relation to the registration and storage by German public authorities of the Internet protocol address of visitors. See: Paul De Hert, 'Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after ***Breyer***' (2017) 3(1) European Data Protection Law Review 20; Case C-582/14 ***Patrick Breyer v Bundesrepublik Deutschland*** [2016] OJ C475/3. For Mr Patrick Breyer's profile, see: Patrick Breyer, 'About Me' (Patrick Breyer) <https://www.patrick-breyer.de/?page_id=573913&lang=en> accessed 17 May 2020; European Parliament, 'Patrick BREYER' (European Parliament) <https://www.europarl.europa.eu/meps/en/197431/PATRICK_BREYER/cv> accessed 17 May 2020.

6 Given length of proceedings, their constitutional complaint included the 2007 amendments to section 111 (supra, note 1). ***Breyer***, paras 9-10.

In its 2012 judgment, the Federal Constitutional Court found compliance with the Basic Law and constitutionality of sections 111, 112 and 113.[7] The applicants brought their case before the European Court of Human Rights (ECtHR or the Court) claiming that section 111 violated their right to respect for private life and correspondence as protected under Article 8 of the European Convention on Human Rights (ECHR) and their freedom of expression protected under Article 10 of the ECHR.[8]

1.1 The Article 8, paragraph 1 exercise: protection of data and self-determination

After a long exposé on the findings of the Federal Constitutional Court, followed by relevant legal provisions and background, comes the fifteen-page-long assessment of the ECtHR,[9] accompanied by a dissenting opinion of Judge Ranzoni.[10]

In our opinion, the way the applicants 'set up' their case was far from optimal and allowed the ECtHR some unnecessary discretion in its approach to the case. The ECtHR kicked off with a preliminary remark on the scope of its assessment. Since solely section 111 had been invoked by the applicants, in the view of the Court, the Court limited its analysis to the storage of subscriber data and the right to respect for private life; the assessment covered neither sections 112 and 113 nor alleged interference with the right to respect for correspondence and freedom of expression –possibly entailing the users' right to anonymity.[11] Nevertheless, sections 112 and 113 were, to the ECtHR, relevant for the proportionality test.[12] Thereafter, the Court moved on to the merits. It, first, highlighted the broad concept of privacy and "private life" protected by Article 8 ECHR.[13] The notion of "private life" was given a broad interpretation, allowing the ECtHR to establish a close connection between the right to privacy and the right to the protection of personal data.[14] Moreover, data collection or otherwise processing can, to the Court, function as a threat to

7 ***Breyer***, para 12. The Federal Constitutional Court found interference with the right to informational self-determination. It, first, assessed section 111, which was, to the court, aimed at the legitimate goal of criminal prosecution. Though precautionary, the collection and storage of data under section 111 were justified in the light of the limited nature of information gathered and retained; this limited nature also satisfied proportionality in the narrow sense (***Breyer***, paras 14-16). Before addressing sections 112 and 113, the Federal Constitutional Court presented the "double door" concept of data exchange, entailing a "door" of transfer and a "door" of retrieval. The court found that both of these doors have an independent legal basis and must be (separately) opened for data exchange to occur. On one hand, there is data transfer: a service provider, who has a duty to collect/store (section 111), make available (section 112) and provide on demand (section 113) subscriber data, supplies these data. On the other hand, there is data retrieval: the agency seeks these data and the empowered authorities have the right to retrieve them via the automated request (section 112) or on demand (section 113). For the latter case of retrieval, an additional legal basis in federal or Länder law is demanded (***Breyer***, para 14 with references to paras 123-125 of the judgment of the Federal Constitutional Court). Having explained this concept, the Federal Constitutional Court considered section 112 as enabling data transmission, but not collection (***Breyer***, paras 17-18). On proportionality, section 112 was found suitable and necessary, because it enhanced effectiveness in pursuing the legitimate goals referred to in the exhaustive list of that section (***Breyer***, para 19). Proportionality in the narrow sense was also met, since various balancing factors favoured access: for instance, the number of the empowered authorities was limited, purposes pursued were related to security and data as such had limited probative value (***Breyer***, para 19). Finally, section 113, the "release provision" according to the "double door" concept, demanded an additional legal basis for the retrieval of data to occur (***Breyer***, para 20). Despite lack of an exhaustive list in relation to entitled authorities, section 113 was deemed constitutional, in light of the restricted nature of data initially collected and stored (***Breyer***, paras 20-21).-

8 ***Breyer***, para 59.

9 The examination of the applicants' claims starts at paragraph 59.

10 We refer to Judge Ranzoni's Opinion where necessary throughout our analysis. ***Breyer***, Dissenting Opinion of Judge Ranzoni.

11 ***Breyer***, paras 60-63, in particular para 62 ("(…) The Court is therefore not called in the present case to decide if and to what extent Article 10 of the Convention maybe be considered as guaranteeing a right for users of telecommunication services to anonymity (…) and how this right would have to be balanced against others imperatives (…)").

12 ***Breyer***, para 60.

13 ***Breyer***, para 73 ("(t)he Court reiterates that private life is a broad term not susceptible to exhaustive definition").

14 ***Breyer***, para 74 ("(…) In the context of personal data, the Court has pointed out that the term "private life" must not be interpreted restrictively. It has found that the broad interpretation corresponds with that of the Data Protection Convention, the purpose of which is "to secure in the territory of each Party for every individual (…) respect for his rights und fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (…)").

self-determination of citizens whose data are collected; hence, the right to informational self-determination can be protected under Article 8 of the ECHR (under the scope of "private life").[15] In this context, the Court held that (the mere) storage of subscriber data under section 111 interfered with the applicants' right to respect for "private life".[16] Subscriber data can be covered by the right to informational self-determination, since, in the light of potential correlations, no personal datum is "in itself, that is, regardless of the context of its use, insignificant".[17] Paragraph 1 of Article 8 of the ECHR was, thus, applicable to the case at hand.[18]

1.2 The Article 8, paragraph 2 exercise: a three-prong necessity test: pressing social need, suitability and proportionality

The Court then turned to examine paragraph 2 of Article 8 of the ECHR[19] and, in particular, the threefold test of legality, legitimacy and necessity. The German legal system passed the legality test. The interference at issue (storage) was based on domestic law (section 111) that was, to the ECtHR, adequately accessible, clear and foreseeable.[20] At this point, the Court postponed the examination of the "quality of law"-criterion, referring to safeguards in law protecting from abuse or misuse of data. The assessment of such safeguards was, to the ECtHR, closely linked to the issues of access to and use of data by relevant authorities. Thus, the Court held that this analysis was, under these circumstances, primarily connected with the necessity test, which should moreover address sections 112 and 113 regulating such access and use.[21] Regarding legitimacy, the interference was, to the ECtHR, aimed at the goals of "public safety, prevention of disorder or crime and the protection of the rights and freedoms of others".[22] We will come back to this strategy of fusing two different tests in our comments ***below.***

15 ***Breyer***, para 75 ("(…) It further follows from the Court's well-established case-law that where there has been a compilation of data on a particular individual, the processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged (…)").

16 ***Breyer***, para 81 ("(…) It is not contested by the parties that the obligation for service providers to store personal data in accordance with section 111 of the Telecommunications Act interfered with the applicants' right to respect for their private life, since their personal data were stored. In this respect the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the Convention (***Leander v. Sweden***, 26 March 1987, § 48, Series A no. 116) (…)").

17 ***Breyer***, para 81 ("(…) It takes furthermore note of the Federal Constitutional Court's finding that the extent of protection of the right to informational self-determination under domestic law was not restricted to information which by its very nature was sensitive and that, in view of the possibilities of processing and combining, there is no item of personal data which is in itself, that is, regardless of the context of its use, insignificant (…)").

18 ECHR, art 8(1) ("(…) Everyone has the right to respect for his private and family life, his home and his correspondence (…)").

19 ECHR, art 8(2) ("(…) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (…)").

20 It contained, for instance, clear provisions on duration and conditions of storage. ***Breyer***, paras 83-84.

21 ***Breyer***, para 85 ("(…) In so far as safeguards, access of third parties and further use of the stored data are concerned section 111 of the Telecommunications Act has to be read in conjunction with its sections 112 and 113 and, according to the 'double door concept' explained by the Federal Constitutional Court (…), in conjunction with the relevant legal basis for individual information requests. The Court considers, however, that the question of foreseeability and sufficient detail of these provisions are in the present case closely related to the broader issues of whether the interference was necessary in a democratic society and proportionate. It will therefore further assess them when it comes to those issues (…)").

22 It is noteworthy that, when determining the legitimate goals pursued by storage under section 111, the ECtHR drew particular attention to the goals of data requests (regulated by sections 112 and 113), as well as the criminal aspects of the above legitimate goals. ***Breyer***, para 87 ("(…) In this connection the Court notes the explanation of the Federal Constitutional Court's judgment that access to the information stored is for "the purpose of warding off dangers, prosecuting criminal offences or regulatory offences and performing intelligence duties" (…) These purposes are further emphasized in the Telecommunications Act, which states that information requests are permissible in so far as they are necessary to prosecute criminal and regulatory offences, to avert danger and to perform intelligence tasks (…)").

Moving on to the necessity test, the Court stressed that the storage in question could be "necessary in a democratic society", if it addressed a "pressing social need" and if it were proportionate to the above-detected legitimate goals.[23] A closer look of the paragraphs that follow reveals that the Court tests not two, but three elements when addressing necessity: first, pressing social need; second, suitability of the interference; and, third, proportionality (whether the interference was proportionate to the aims pursued), including a balancing exercise, where the Court looked for safeguards and review possibilities.

- The fight against crime and the protection of the people, especially in light of new types of crime and terrorism, were, to the Court, the demanded "pressing social need".[24] Therefore, the first limb of the three-prong test was satisfied.
- On suitability, the Court saw telecommunications-related technology as a crucial investigative tool, necessary for law enforcement authorities to combat crime.[25] In this context, it accepted the government's claim that storage was an effective measure assisting authorities in the fight against crime.[26] Moreover, the comparative analysis demonstrated that there was no consensus amid states regarding the storing of subscriber data in particular relation to SIM cards; such lack of consensus enlarged the margin of appreciation held by domestic authorities in choosing the appropriate response to technological developments.[27] Hence, to the Court, storage, under section 111, was a suitable response to telecommunication-related advances;[28] it did address the above-identified pressing social need.
- The ECtHR then proceeded to the third limb of the necessity test, i.e. proportionality: is the interference proportionate to the above-detected legitimate goals. This part of the reasoning consists of two steps. First step: assessing the seriousness of the contested German measure. Second step: balancing of means and end in the light of existing safeguards and review possibilities. Both steps will be discussed in the following sections.

1.3 The importance of safeguards to assess proportionality: charmed by German "double door" concept of data exchange

The Court, first, determined the level of the interference with the applicants' right to respect for private life. It compared the ***Breyer***-case with data-related case law. Contrary to previous cases, ***Breyer*** (as the Court held) dealt solely with storage (not further uses)[29] of subscriber data (not location or traffic data)[30] that

23 ***Breyer***, para 88.
24 ***Breyer***, para 88.
25 ***Breyer***, para 88 ("(…) It also recognises that modern means of telecommunications and changes in communication behaviour require that investigative tools for law enforcement and national security agencies are adapted (…)").
26 This effectiveness could, to the Court, not be diminished by the risk of registering false data or using second-hand SIM cards, as had been argued by the applicants. ***Breyer***, paras 89-90 ("(…) The Court acknowledges that pre-registration of mobile-telephone subscribers strongly simplifies and accelerates investigation by law-enforcement agencies and can thereby contribute to effective law enforcement and prevention of disorder or crime (…) the existence of possibilities to circumvent legal obligations ("by submitting false names or using stolen, second-hand or foreign SIM cards", as claimed by the applicants in paragraph 89) cannot be a reason to call into question the overall utility and effectiveness of a legal provision (…)"; text in parenthesis ours).
27 ***Breyer***, paras 58, 90.
28 ***Breyer***, para 90.
29 ***Breyer***, para 92, with references to: ***Dimitrov-Kazakov v Bulgaria*** Applicationno 11379/03 (ECtHR, 10 February 2011); ***Shimovolos v Russia*** Application no 30194/09 (ECtHR,21 June 2011).
30 ***Breyer***, para 93, with references to the CJEU's case law: Joined Cases C-293/12 and C-594/12 ***Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others*** [2014] OJ C175/6 (***Digital Rights Ireland***); Joined Cases C-203/15 and C-698/15 ***Tele2 Sverige AB (C-203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v Tom Watson, Peter Brice, Geoffrey Lewis*** (Grand Chamber, 21 December 2016) [2017] OJ C53/11 (***Tele2 Sverige***).

were of limited nature (neither "highly personal" nor targeted at profiling).[31] The most relevant case was, to the ECtHR, the CJEU's ***Ministerio Fiscal***-judgment.[32] In this latter case, access to information was not considered as serious interference, because data correlations could not reveal further information – duration of communications for example. On this basis, the interference caused by the storage at issue was found "while not trivial, of a rather limited nature".[33]

Thereafter, the proportionality assessment focused on safeguards and review procedures.

German law offered plenty of safeguards in the view of the Court. On section 111, whose "technical" safeguards had not been doubted by the applicants,[34] the ECtHR held that duration of storage did "not appear inappropriate", especially in the light of often-lengthy periods of investigations, and that data stored were limited to what was necessary to identify the subscriber.[35] Aside from section 111's storage-related safeguards, the Court examined the issues of access to and use of data by authorities. This was something we expected: during the legality test, the Court had postponed the testing of the "quality of law"-criterion to address it here in the necessity test in relation to, not only section 111 but also, sections 112 and 113 governing access and use.[36] In fact, given the risk of potential future uses of data, the Court found it relevant to address the very legal basis for such access and use.[37]

On section 112, the Court reiterated the automated and centralised nature of the retrieval procedure, which furthermore facilitated ready availability of information stored.[38] Such automation, centralisation and availability could, to the ECtHR, create risks for data stored; albeit, (the Court held) section 112's exhaustive list of authorities empowered to request access could to a considerable extent limit interference.[39] This was the case, because, to the ECtHR, all enlisted authorities were related solely to "law enforcement or the protection of national security".[40] Regarding section 113, despite its lack of an exhaustive list of authorities, its detailedness made it foreseeable as to which authorities may request access to data stored.[41]

31 ***Breyer***, para 92, citing case law on metering data (such as ***Malone*** or ***Copland***), geolocation data (involved in ***Uzun***) or sensitive data (like DNA-related information retained in ***Marper***). ***Malone v the United Kingdom*** Application no 8691/79 (ECtHR, 2 August 1984) (***Malone***); ***Copland v the United Kingdom*** Application no 62617/00 (ECtHR, 3 April 2007) (***Copland***); ***Uzunv Germany*** Application no 35623/05 (ECtHR, 2 September 2010) (***Uzun***); ***S and Marper v the United Kingdom*** Applications nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) (***Marper***).

32 ***Breyer***, para 94, citing Case C-207/16 ***Ministerio Fiscal*** [2018] OJ C436/2 (***Ministerio Fiscal***).

33 ***Breyer***, para 95.

34 ***Breyer***, para 96 ("(…) the Court observes that the applicants have not alleged that the data storage at issue was subject to any technical insecurities (…)").

35 ***Breyer***, para 96.

36 The considerations of the Court on the connection between the examination of safeguards and the necessity test are in: ***Breyer***, para 85.

37 ***Breyer***, para 97 ("(…) The Court agrees with the parties that, in the present case, it cannot consider the proportionality of the interference without closely assessing the future possible access to and use of the data stored.
Therefore, it finds it of relevance to consider the legal basis for information requests and the safeguards available (…)").

38 ***Breyer***, para 29 and accompanying text of section 112 of the Telecommunications Act (see ANNEX).

39 ***Breyer***, para 98.

40 ***Breyer***, para 98 ("(…) the fact that the authorities which can request access are specifically listed in section 112 of the Telecommunications Act constitutes a limiting factor. Even though the list appears broad, all authorities mentioned therein are concerned with law enforcement or the protection of national security (…)").

41 ***Breyer***, para 99 ("(…) the information retrieval is not simplified to the same extent as under section 112, since the authorities have to submit a written request for the information sought (…) the authorities entitled to request access (…) are identified with reference to the tasks they perform but are not explicitly enumerated. While the Court considers this description by task less specific and more open to interpretation, the wording of the provision nonetheless is detailed enough to clearly foresee which authorities are empowered to request information (…)").

In its assessment of the safeguards, the Court relied upon the German Federal Constitutional Court's "double door" concept of data exchange that required one "door" to be opened for the transfer of data stored and another "door" to be opened for the retrieval of these data.[42] In the former case, the door could open when data were released by the service provider or the Federal Network Agency; in the latter case of retrieval, an additional legal basis in federal or Länder law was demanded for the door to open.[43] This "double door" concept was, to the Court, an important safeguard against abuses of data stored.[44] In addition, information was, to the ECtHR, limited to what was necessary[45] and subject to erasure rules.[46] These elements led to the finding that limitations to requests were sufficient.[47]

1.4 The importance of review to assess proportionality: identifying pre-paid card users is too minor to apply the regular three-level test

As said, in its assessment of proportionality, the Court not only looked at safeguards, but equally at review possibilities and supervision of requests. In the eyes of the Court, the examination of review and supervision in general is about a three-level testing: when interference "is first ordered, while it is being carried out, or after it has been terminated".[48] Among these phases, it is the former two that may involve unawareness of the surveilled and that, for this reason, require enhanced procedural safeguards.[49]

However, the ECtHR here announced that this general three-level test, thus far applied to more intrusive types of interference (mainly in surveillance contexts), could not be applied to the contested German measures in this case that were not that intrusive; the Court hence opted for a more flexible standard,[50]

42 See supra, note 7; ***Breyer***, para 100, in conjunction with para 14 (referring to para 125 of the judgment of the Federal Constitutional Court).

43 See supra, note 7; ***Breyer***, para 100, in conjunction with para 14 (referring to para 125 of the judgment of the Federal Constitutional Court).

44 ***Breyer***, para 100 ("(…) Concerning both provisions, the Court observes that the stored data is further protected against excessive or abusive information requests by the fact that the requesting authority requires an additional legal basis to retrieve the data. As explained by the Federal Constitutional Court through its double door comparison (…), sections 112 and 113 (…) only allow the Federal Network Agency or the respective service provider to release the data. However, a further provision is required to allow the specified authorities to request the information (…)"). It is expressly added that (in a similar case) in the recent Order of 27 May 2020 (1 BvR 1873/13, 1 BvR 2618/13), the First Senate of the Federal Constitutional Court found unconstitutionality of the aforementioned section 113. To the First Senate, even though the interference at hand was not of significant gravity, for the transferring and retrieving of subscriber data (double door concept in the context of maintaining public security and the activities of intelligence services), there was a prerequisite of concrete danger (to be warded off) in the individual case, as well as suspicion of engagement in a criminal offence (regarding investigation and prosecution). In the absence of the requirement of concrete danger, more rigorous safeguards had to be in place to balance relevant legal stakes. See in more detail: Bundesverfassungsgericht, 'Legal provisions on providing and obtaining information on subscriber data are unconstitutional - Press Release No. 61/2020 of 17 July 2020' (Bundesverfassungsgericht, 17 July 2020) <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-061.html> accessed 21 July 2020.

45 For instance, in prosecution contexts initial suspicion was required as a minimum. ***Breyer***, para 100.

46 Erasure rules could apply, where data were no longer needed. ***Breyer***, para 100.

47 The Court explicitly added that the limitation of data stored to what was necessary was further supported by European and domestic data protection laws (***Breyer***, para 100). Moreover, the ECtHR took into account that data requests under section 113's written procedure were fewer than those under section 112's automated process; this demonstrated that the written procedure worked as a disincentive for authorities to access and use data in cases where such access and use were not truly necessary (***Breyer***, para 101).

48 ***Breyer***, para 102, citing ***Klass and Others v Germany*** Application no 5029/71 (ECtHR, 6 September 1978) (***Klass***).

49 ***Breyer***, para 102, citing ***Klass***.

50 ***Breyer***, para 103 ("(…) (t)he Court observes, however, that all these cases concerned individualised and more serious and intrusive interferences with the right to respect for private life that cannot be transferred to the access of data in the present case. In sum it considers that the level of review and supervision has to be considered as an important, but not decisive element in the proportionality assessment of the collection and storage of such a limited data set (…)").

and satisfied itself by the following elements: responsibility borne by the retrieving agency regarding legality of requests, in conjunction with competence of the Federal Network Agency with regard to admissibility of a given transmission;[51] documentation of retrievals and overall supervision of such retrievals by the independent Federal and Länder data protection authorities that could moreover guarantee the opportunity to appeal;[52] general rules of domestic law offered further opportunities to contest retrievals;[53] and, in any event, given these chances to challenge relevant decisions, the absence of notification and the secrecy engulfing retrievals did not amount to violation of Article 8 of the ECHR.[54] This type of supervision met the flexible threshold of review by an independent authority.

Before reaching conclusions, the Court reminded the lack of consensus among states regarding the collection and storage of subscriber data; this absence of agreement justified a wider margin of appreciation for the German authorities in regulating storage of subscriber data to protect national security and combat crime.[55]

Overall, the interference was deemed proportionate to the aim pursued; hence, the storage of subscriber data by the service providers, under section 111, was deemed necessary in a democratic society.[56]

2. Comments

2.1 Intertwining or mixing tests may provide judges with safety, but can have side-effects

Breyer is yet another judgement in which the Court intertwines the legality and necessity test. We briefly observed in the forgoing that the Court, after finding that storage of subscriber data under section 111 constitutes an interference with a legal basis, found that the German law was sufficiently accessible and foreseeable,[57] albeit it postponed the "quality of law"-assessment that is, as a rule, part of the legality test.

51 ***Breyer***, para 104 ("(…) in principle under section 113 of the Telecommunications Act its paragraph 2 clarifies that the responsibility for the legality of the information request lies with the retrieving agency and that the telecommunication providers have no competence to review the admissibility of any request, as long as the information is requested in written form and a legal basis is invoked. Under section 112 of the Telecommunications Act, however, the Federal Network Agency is competent to examine the admissibility of the transmission when there is a special reason to do so (…)").

52 ***Breyer***, para 105 ("(…) each retrieval and the relevant information regarding the retrieval (…) are recorded for the purpose of data protection supervision. This supervision is conducted by the independent Federal and Länder data protection authorities. The latter are not only competent to monitor compliance with data protection regulation of all authorities involved but they can also be appealed to by anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies (…)").

53 ***Breyer***, para 106 ("(…) the Court notes that the Federal Constitutional Court held that legal redress against information retrieval may be sought under general rules (…) – in particular together with legal redress proceedings against the final decisions of the authorities (…)").

54 ***Breyer***, para 107 ("(…) (t)he Court considers that the possibility of supervision by the competent data protection authorities ensures review by an independent authority. Moreover, since anyone, who believes his or her rights have been infringed, can lodge an appeal the lack of notification and confidentiality of the retrieval procedure does not raise an issue under the Convention (…)").

55 ***Breyer***, para 108.

56 ***Breyer***, para 109.

57 ***Breyer***, paras 83-84.

The "quality of law"-assessment, related to safeguards that protect against abuse or misuse of information, is, to the Court, more strongly connected with the necessity test.[58] In its data privacy-related case law and where the circumstances of the case allow so, the Court tends to detach the "quality of law"-assessment from the legality test and to incorporate it into the necessity test.[59]

Since safeguards in law are now examined in the context of the proportionality assessment, this mixing-technique can constitute a safer exercise for the Court: instead of addressing straight proportionality questions, such as "is the storage of subscriber data appropriate?" or "is it the least harmful means?", the ECtHR simply looks for safeguards in the law. Even though this intertwining may provide judges with safety, it could have side-effects. In the case at hand, the Court seems to scrutinise section 111 as such (in abstracto),[60] as well as to peruse detailedness and foreseeability of sections 112 and 113 that were never invoked by the applicants.[61] More importantly, and in addition to this in abstracto or of its own motion examination of the law, the legality/necessity mix can affect the quality of the Court's reasoning. This can be demonstrated by the findings on safeguards of sections 112 and 113; the Court "discovers" safeguards that are actually ***not*** present in these sections, but to be found in other legal provisions of federal or Länder law.[62]

2.2 In the past, the Court already accepted watered down-versions of the strict approach to legality in Huvig

Since, at least, the nineteen-eighties, the ECtHR has developed a well-structured approach to the legality

58 ***Breyer***, para 85.

59 See among others: ***Marper***, para 99; ***Gaughran***, para 73 (citing ***Marper***); ***MK v France*** Application no 19522/09 (ECtHR, 18 April 2013) (***MK v France***), para 28 (citing ***Marper***). This intertwining has brought new safeguards in surveillance contexts. For example, the ***Zakharov***-judgment mixed foreseeability with necessity and examined: "accessibility of the domestic law"; "the scope and duration of the secret surveillance measures"; "the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data"; "the authorisation procedures"; "the arrangements for supervising the implementation of secret surveillance measures"; and "any notification mechanisms and the remedies provided for by national law". ***Roman Zakharov v Russia*** Application no 47143/06 (ECtHR, 4 December 2015) (***Zakharov***) paras 237-238.

60 ***Breyer***, Dissenting Opinion of Judge Ranzoni, para 7.

61 ***Breyer***, para 99, referring to foreseeability as to which authorities may request access to data stored.

62 It is reminded that these sections refer to data exchange, entailing data transfer and data retrieval. On one hand, the service provider, collecting/storing, making available and providing on demand subscriber data (under sections 111, 112 and 113 respectively), supplies these data; and, on the other hand, the agency seeks these data and the empowered authorities retrieve them via the automated request or on demand (under sections 112 and 113 respectively). The latter retrieval-scenario demands an additional legal basis in federal or Länder law (***Breyer***, para 100, in conjunction with para 14 referring to para 125 of the judgment of the Federal Constitutional Court). The piecemeal regulation of data exchange, involving the additional legal basis outside the sections at issue, played an important role in the determination of the existence of sufficient safeguards (***Breyer***, para 100). Yet, this approach is problematic: if the requirements needed are to be found in legal provisions other than the one at issue (section 111), as well as other than the (uninvoked) ones assessed by the Court to determine necessity of storage (sections 112 and 113), then it seems obvious that sections 111, 112 and 113 do not contain these requirements and, hence, suffer insecurities. When the Court looks for safeguards in law to assess the "quality of law" or the "necessity" of a measure, it might be preferable that it actually seeks for such safeguards in the particular legal provision(s), instead of relying upon what is missing from this provision(s) or regulated elsewhere to argue for sufficiency on the grounds of what the law neither expressly prescribes nor explicitly prohibits. Here, an analogy could be drawn with the CJEU-judgment in ***Schwarz***, where the CJEU abstained from thoroughly scrutinising the relevant legal provisions of the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L385/1. Despite risks of centralised storing and of using data, already gathered, for purposes other than verification of authenticity of passport and identity of its holder and even though the Regulation at issue did not explicitly prohibit such central storing and function creep, the CJEU considered the provisions for storage in the passport and for processing for the above verification-goals as adequate safeguards against misuse and abuse. See Case C-291/12 ***Michael Schwarz v Stadt Bochum*** [2013] OJ C367/17 (***Schwarz***), paras 55-61. See a contrario: ***Digital Rights Ireland***, paras 58-68. Here, the CJEU, after thorough scrutiny, did not find adequate safeguards; it found major shortcomings and deficiencies. Relying exactly upon what the Directive 2006/24/EC did ***not*** explicitly prohibit, restrict or provide for (such as clear and precise rules on limitations to retention or access of authorities), the CJEU declared the Directive invalid. See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

test in order to avoid abuses in the exercise of public power. Namely, the 1984 ***Malone***-judgment, dealing with metadata and surveillance by police in criminal investigations, clarified that (surveillance-related) laws need be foreseeable, not as to the likelihood that the authorities may interfere with the people's right to privacy but, as to "the circumstances in which and the conditions on which public authorities are empowered to resort" to such interference.[63] ***Malone***'s legality test required legal provisions be accessible, foreseeable and precise in the sense of sufficiently indicating "the scope and manner of exercise of the discretion conferred on the relevant authorities".[64] Such a test demanded detailedness referring to the why and the how, the overall organisation of the interference (in that case, surveillance).[65]

Malone's legality test was upgraded by the 1990 ***Huvig***-judgment addressing the legal basis of criminal law-related powers.[66] Calling for more intelligent rules to regulate more intelligent technologies,[67] the ***Huvig***-Court required a legal basis for the interference, accessibility of this legal basis, foreseeability as to the consequences and compliance of the whole national structure with the Rule of Law.[68] ***Huvig*** delivered what we have elsewhere referred to as the "minimum foreseeability package"[69] including a number of elements that should be included in the law: the categories of people liable to be surveilled; the nature of the offences that may trigger surveillance measures; limitations on duration of surveillance; the procedures on storing data; the precautions regarding communicating data; the circumstances for erasure of data; as well as judicial control and notification of the surveilled.

Thanks to ***Malone*** and ***Huvig***, the legality test became an almost fully-fledged check of concreteness; it acquired an enhanced detailedness-demand regarding the why and the how of exercising discretion (***Malone***) and a Rule of Law-testing followed by a package of foreseeability minimums (***Huvig***). Could this test be applied to softer cases? Experience has answered in the affirmative, albeit with a caveat: safeguards can be affected, when interference-level is lower.

63 ***Malone***, para 67 ("(…) the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence (…)").

64 ***Malone***, para 70 ("(…) (t)he issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities (…)").

65 A detailed analysis in: Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance: The ECtHR's Expanded Legality Testing Copied by the CJEU' in Valsamis Mitsilegas and Niovi Vavoula (eds), ***Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives*** (Hart 2021) 255, 259-261.

66 ***Huvig v France*** Application no 11105/84 (ECtHR, 24 April 1990) (***Huvig***).

67 ***Huvig***, para 32 ("(…) (t)apping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated (…)").

68 See in more detail: Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance' (supra, note 65) 262 and accompanying Table 10.1.

69 Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance' (supra, note 65) 263 and accompanying Table 10.2.

The 2010 ***Uzun***-judgment, dealing with GPS data (less intrusive than other types of surveillance, like phone tapping), supported a lighter version of the legality test. Here, foreseeability appeared relaxed with less detailedness and general terms favoured over precise ones;[70] concrete rules or precautions on, for instance, treating, sharing or deleting information were absent; and ex ante review and notification, as an effective legal basis subject to the legality test, were replaceable by less effective ex post safeguards,[71] like judicial review or notification, addressable now under the necessity test.[72]

Watered down-versions of ***Malone***'s and ***Huvig***'s approach to legality can also be found in later case law on mass surveillance.[73] For example, the 2006 ***Weber and Saravia***-judgment on secret "strategic monitoring" slightly addressed notification as an ex post safeguard (not to jeopardise secrecy of monitoring) when testing necessity.[74] And, more recently, the 2018 ***Big Brother Watch***-Court was not bothered by having foreseeability prejudiced by independent oversight –of selectors and search factors on bulk data processing that were neither public nor included in the interception-warrant.[75]

70 ***Uzun***, para 63 referring to the "grounds" (rather than the people liable to be subjected to the measure at hand or the types of offences possibly triggering application of the measure) or the "authorities" (rather than a particular public actor): "(…) In addition, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights (…) The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (…)".

71 Milaj has argued for the effectiveness of ex ante regulation and highlighted a number of concerns in relation to ex post safeguards, such as: there may be confusion as to who decides over the matter in question (in light of the separation of powers); authorities may enjoy a wide margin in determining the issue at hand; or, after the fact (for instance, after a serious offence) the balancing exercise would favour more intrusive measures. Jonida Milaj, 'Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance' (2016) 30(3) International Review of Law, Computers & Technology 115, 117 (with further references).

72 ***Uzun***, para 72 ("(…) The Court considers that such judicial review and the possibility to exclude evidence obtained from an illegal GPS surveillance constituted an important safeguard, as it discouraged the investigating authorities from collecting evidence by unlawful means. In view of the fact that GPS surveillance must be considered to interfere less with a person's private life than, for instance, telephone tapping (…), the Court finds subsequent judicial review of a person's surveillance by GPS to offer sufficient protection against arbitrariness. Moreover, Article 101 § 1 of the Code of Criminal Procedure contained a further safeguard against abuse in that it ordered that the person concerned be informed of the surveillance measure he or she had been subjected to under certain circumstances (…)"). A more detailed analysis in: Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance' (supra, note 65) 265-266 and accompanying Table 10.3.

73 For a full analysis of case law involving altered versions of ***Huvig***'s approach to legality, see: Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance' (supra, note 65) 267ff, with further references to, among others, ***Liberty and others v the United Kingdom*** Application no. 58243/00 (ECtHR, 1 July 2008) (***Liberty***); and ***Kennedy v the United Kingdom*** Application no. 26839/05 (ECtHR, 18 May 2010).

74 ***Gabriele Weber and Cesar Richard Saravia v Germany*** Application no. 54934/00 (ECtHR, 29 June 2006) (***Weber and Saravia***), paras 133-136, in particular para 135 ("(…) The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (…) However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. Indeed, such notification might reveal the working methods and fields of operation of the Intelligence Service (…) As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (…)").

75 ***Big Brother Watch and Others v The United Kingdom*** Application nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), paras 338-347, especially para 340 ("(…) This does not mean that selectors and search criteria need to be made public; nor does it mean that they necessarily need to be listed in the warrant ordering interception. In fact, in the ***Liberty*** proceedings the IPT found that the inclusion of the selectors in the warrant or accompanying certificate would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic" (…) The Court has no reason to call this conclusion into question. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight (…)").

Such alterations of the otherwise strengthened legality test could mean that ***Huvig*** is not always a point of reference, but a mere source of inspiration. This is especially true for softer cases. In this regard, ***RE*** stressed that what matters is the impact on privacy, not the technology used; in low-level cases of intrusion, the ***Huvig***-perspective, though not directly applicable, may serve as an inspiration.[76]

2.3 Breyer is just another of these watered down-versions relying mainly on ex post controls

This brings us to ***Breyer*** that seems to reflect the above developments in and watering down of the legality test. When embedding legality into necessity, the ***Breyer***-Court finds that the storage of subscriber data amounts to a rather limited interference.[77] This is, thus, a soft case. On safeguards, the assessment is limited to the duration of the interference (which, we remind, is "storage" of subscriber data under section 111), as well as the limited scope of this interference to what is necessary for the identification of the subscriber.[78] Then, silence. The Court moves on to safeguards relating to access and use under sections 112 and 113 (that is, beyond storage). It finds adequate protection against abuse of data stored, because of section 112's exhaustive list (of empowered authorities), section 113's detailedness (that is of a lower level, in light of absence of its own exhaustive list) and the double door-concept.[79] Last, the Court addresses review of requests (not of storage) and is satisfied by ex post guarantees, like appeal opportunities granted by general or data protection legal provisions.[80]

Therefore, in ***Breyer***, we miss ***Malone***'s augmented detailedness of the why and the how of the exercise of discretion, as well as ***Huvig***'s Rule of Law-compliance and fully-fledged package of minimum foreseeability; and we miss this with regard to section 111. We do find ***Uzun***'s low-levelled detailedness accompanied by (***Uzun***'s and ***Weber and Saravia***'s) transformation of ex ante safeguards, considered under the legality test, into ex post guarantees, addressed through necessity; but we find this with regard to sections 112 and 113, not section 111.[81] Overall, we observe that, as was the case with ***Big Brother Watch***, (ex post) control wins, foreseeability fails.

By mixing necessity with legality and, thus, favouring ex post regulation over overall regulation (including ex ante), the Court over-engages in questions of an after-the-interference-type (like, "is the review independent in light of the opportunity to lodge a complaint?") and does not address questions of essence

76 ***RE v the United Kingdom*** Application no. 62498/11 (ECtHR, 27 October 2015) (***RE***), paras 129-130 ("(…) In ***Uzun v. Germany*** (…) the Court accepted that the monitoring of a car's movements by GPS interfered with the applicant's Article 8 rights. However, it distinguished this kind of surveillance from other methods of visual or acoustic surveillance which were generally more susceptible of interfering with Article 8 rights because they disclosed more information on a person's conduct, opinions or feelings. Therefore, the Court indicated that, while it would not be barred from drawing inspiration from the principles set up and applied in the specific context of surveillance of telecommunications, those principles would not be directly applicable in a case concerning surveillance of movements in public places via GPS because such a measure "must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations". Instead, the Court applied the more general principles on adequate protection against arbitrary interference with Article 8 rights (…) The Court has not, therefore, excluded the application of the principles developed in the context of interception cases in covert-surveillance cases; rather, it has suggested that the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference (…)").

77 ***Breyer***, para 95 ("while not trivial, of a rather limited nature").

78 ***Breyer***, para 96.

79 ***Breyer***, paras 97-100.

80 ***Breyer***, paras 102-107.

81 See for example: ***Breyer***, para 107 ("(…) (t)he Court considers that the possibility of supervision by the competent data protection authorities ensures review by an independent authority. Moreover, since anyone, who believes his or her rights have been infringed, can lodge an appeal the lack of notification and confidentiality of the retrieval procedure does not raise an issue under the Convention (…)").

with regard to the very initial stage of collection and storage. If service providers are by law (section 113) not the ones responsible for the legality of requests and if the agency retrieving data stored is the one to be held accountable for such legality,[82] then the questions seem to be: Can the scrutiny of requests by the agency be considered as independent supervision of the interference at issue (meaning storage)? Is the checking of admissibility of transmission (under section 112) by the agency enough to satisfy independent review at earlier stages when the subscriber is unaware of the interference? Can this be the case, where public entities may escape major accountability-demands, like transparency, under the European Union law[83] that the ECtHR relies upon[84] to support its sufficiency-conclusions? Such questions are not addressed by the ***Breyer***-Court.

2.4 A reminder of necessity/proportionality testing in Germany/ Luxembourg and Strasbourg

The mixing of questions about legality and necessity not only thwarts the general idea that surveillance should be checked not only afterwards, but also during and before (see ***above),*** but also has a strange effect on the legal practitioners' common understanding of the necessity or proportionality test. To better explain this observation, we need to recall some fundamentals about necessity or proportionality testing in Europe.

Let us recall that the proportionality principle has its roots in the German jurisdiction.[85] As developed in the European Union's law and doctrine, the proportionality assessment typically entails a three-step test examining suitability (whether the measure is suitable, appropriate to reach the aim pursued); necessity/ alternatives (whether the measure is necessary, the least restrictive to achieve this aim); and proportionality in the strict (narrow) sense (whether the measure imposes a burden that is excessive having regard to the aim pursued).[86]

In the Europe of the Council of Europe, when the ECtHR assesses whether a measure is "necessary in a democratic society", the testing is sometimes broader, sometimes narrower compared to the German/

82 ***Breyer***, para 104.

83 Namely, the Data Protection Directive for Police and Criminal Justice Authorities, targeted at public functions, introduces a flexible and public authority-friendly scheme, lacking the principle of transparency, affecting the principles of data minimisation and purpose limitation and imposing limitations on the people's rights. See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Data Protection Directive for Police and Criminal Justice Authorities), art 3(7) (for the focus on public functions); art 4(1)(a), in conjunction with General Data Protection Regulation, art 5(1)(a) (for lack of transparency); art 4(1)(b) and (c), in combination with General Data Protection Regulation, art 5(1)(b) and (c) (for the data minimisation and purpose limitation principles). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation). See also: European Union Agency for Fundamental Rights and Council of Europe, ***Handbook on European Data Protection Law*** (2018 edn, European Union Agency for Fundamental Rights and Council of Europe 2018) 282.

84 ***Breyer***, para 100 ("(…) (t)he Court accepts that there are sufficient limitations to the power to request information and that the requirement of "necessity" is not only inherent in the specific legal provisions subject of this complaint but also to German and European data-protection law (…)").

85 Paul Craig and Gráinne de Búrca, ***EU Law: Text, Cases, and Materials*** (6th edn, Oxford University Press 2015) 551.

86 Paul Craig and Gráinne de Búrca, ***EU Law*** (supra, note 85) 551; Robert Schütze, ***An Introduction to European Law*** (2nd edn, Cambridge University Press 2015) 204-205. See further literature supporting these three steps: Moshe Cohen-Eliya and Iddo Porat, 'American balancing and German proportionality: The Historical Origins' (2010) 8(2) International Journal of Constitutional Law 263, 267; Yutaka Arai-Takahashi, 'Proportionality – A German Approach' (1999) 19 Amicus Curiae 11, 12. For the CJEU's case law on these three steps, see: Case C-343/09 ***Afton Chemical Limited v Secretary of State for Transport*** [2010] OJ C234/14, para 45 (with further references).

Union testing of proportionality. As a rule, one would expect in Strasbourg a broader approach for the simple reason that the testing is about necessity and that proportionality is only one ingredient of this necessity, but there is not always more, on the contrary, sometimes there is less. On the one hand, the Court may assess whether a measure addresses a pressing social need and, more concretely, whether "it is proportionate to the legitimate aim pursued" and whether "the reasons adduced by the national authorities to justify it are "relevant and sufficient"".[87] We have witnessed the application of this broader version in cases like ***Marper*** or ***Segerstedt-Wiberg***.[88] On the other hand, a narrower version of the test is also commonly used, for instance, omitting the "pressing social need"-question or "relevant and sufficient reasons"-element, like in ***Breyer***.[89] A rule of thumb teaches us that the Strasbourg Court does not theorise a lot about its levels of scrutiny.

Then, there is the unique Strasbourg feature of the margin of appreciation. While states can enjoy a certain or considerable margin in identifying the pressing social need and determining the measure-response to this need, this margin (as the Court has made clear) can depend on two specific factors: namely, the concrete goal pursued and the level of the interference at hand.[90] Therefore, intrusiveness of a measure can affect the margin of national authorities to bring privacy-diminishing measures. Such a varying margin can then have an impact on the necessity test –and proportionality therein. For instance, the goal of striking down terrorism could justify a broader margin and, therefore, a looser (legality, legitimacy and) necessity testing; whereas the testing can be stricter in the light of high-levelled intrusiveness.[91] To this, we expressly add legal uncertainty deriving from the oft-used factors accompanying the application of the margin concept: that is, the balancing exercise (importance of individual right versus importance of the limitation) and the consensus amid states. Balancing is exercised on a case by case basis and lacks clear standards applicable to each and every scenario; and lack of clarity on what "consensus" means could result in looking for (social) trends, instead of an agreement upon the particular (legal) measure that is at stake.[92]

87 Among many authorities: ***Lustig-Prean and Beckett v the United Kingdom*** Applications nos 31417/96 and 32377/96 (ECtHR, 27 September 1999), paras 80-81 ("(…) (a)n interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a pressing social need and, in particular, is proportionate to the legitimate aim pursued (…) the Court would underline the link between the notion of "necessity" and that of a "democratic society", the hallmarks of the latter including pluralism, tolerance and broadmindedness (…) (t)he Court recognises that it is for the national authorities to make the initial assessment of necessity, though the final evaluation as to whether the reasons cited for the interference are relevant and sufficient is one for this Court (…)"); ***Coster v the United Kingdom*** Application no 24876/94 (ECtHR, 18 January 2001), para 104 ("(…) (a)n interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued. While it is for the national authorities to make the initial assessment of necessity, the final evaluation as to whether the reasons cited for the interference are relevant and sufficient remains subject to review by the Court for conformity with the requirements of the Convention (…)"); ***Marper***, para 101 ("(…) (a)n interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient" (…)"); ***Nada v Switzerland*** Application no 10593/08 (ECtHR, 12 September 2012), para 181.

88 ***Marper***, para 101; ***Segerstedt-Wiberg and others v Sweden*** Application no 62332/00 (ECtHR, 6 June 2006) (***Segerstedt-Wiberg***), para 88.

89 ***Breyer***, para 88 ("(…) An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and if it is proportionate to the legitimate aim pursued (…)").

90 ***Segerstedt-Wiberg***, para 88 ("(…) the Court considers that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved (…)").

91 On the possible impact of the margin concept on surveillance-testing, see: Paul De Hert and Gianclaudio Malgieri, 'One European Legal Framework for Surveillance' (supra, note 65) 276-278 and accompanying Table 10.5.

92 In this context, Brauch, referring to morals-related case law, has argued that the Court seems to have been motivated by a social agenda, rather than having engaged in legal or textual analysis of the ECHR. Jeffrey Brauch, 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law' (2004) 11 Columbia Journal of European Law 113, 147ff.

In light of the above considerations, the possible elements of the Strasbourg's necessity test can be: first, the "pressing social need"[93] that is not always mentioned by the Court; second, the element of "sufficient and relevant reasons"[94] that seems to be applied when testing is stricter;[95] third, the "least harmful means" (to achieve goal pursued) that is very seldom used;[96] and, fourth, proportionality of the measure to the legitimate aim pursued.[97] Again, the Court does not conceptualise this testing in such a particular way; albeit, the above four elements can occur, with the fourth element of proportionality being the baseline that is, more or less often, complemented with the "pressing social need" and the "relevant and sufficient reasons" and, rarely, with the "least harmful means".

It is noted that the Luxembourg Court's approach is not fundamentally different. Any differences seem to stem from the two texts: Article 8(2) of the ECHR[98] versus Article 52(1) of the Charter.[99] More fundamental is the CJEU's settled case law focusing on the aforementioned German-based version of the proportionality-test requiring that laws be "appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives".[100] This perspective complies with the text of Article 52(1) of the Charter: "(s)ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

93 As, for example, found in ***Breyer***, para 88.

94 See for instance: ***Marper***, para 101; ***Segerstedt-Wiberg***, para 88.

95 This seems to be true in light of the very notion of "relevance" and "sufficiency", requiring a particular link between a premise/matter of evidence and an inference/conclusion. As a matter of evidence, "relevance" has been addressed as "the relationship between two facts that renders one more or less probable from the existence of the other, either taken by itself or in connection with other facts" ('relevance', ***A Dictionary of Law*** (9th edn, Oxford University Press 2018)). As a premise to develop an argument, "relevance" is related to reasoning: a "premise is relevant if its acceptance provides some reason to believe, counts in favor of, or has some bearing on the truth or merit of the conclusion" (Edward Damer, ***Attacking Faulty Reasoning - A Practical Guide to Fallacy-Free Arguments*** (7th edn, Cengage Learning 2013) 33). In law, "relevance" goes beyond logic and common sense and demands probative value (Paul Roberts and Adrian Zuckerman, ***Criminal Evidence*** (Oxford University Press 2010) 99ff). On the other hand, "sufficiency" deals with justification of the acceptance of an argument. A person "making an argument should provide reasons that are sufficient to justify the acceptance of his or her conclusion (…) Are the reasons provided enough to drive to the arguer's conclusion? (…) Is the premise based on insufficient evidence or faulty causal analysis? (…) Is some key or crucial evidence missing that must be provided in order to accept the argument? (…)". A discussion on the principles (structure, relevance, acceptability, sufficiency and rebuttal) of developing an argument in: Ameet Ranadive, 'The 5 Principles of Good Argument' (Medium, 6 January 2018) <https://medium.com/@ameet/the-5-principles-of-good-argument-63d394ca3051> accessed 17 May 2020.

96 For a general discussion, see: Paul De Hert, 'Balancing Security and Liberty Within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11' (2005) 1(1) Utrecht Law Review 68, 80ff, 93ff (with further references).

97 See for example: ***Breyer***, para 88.

98 "(…) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (…)".

99 "(…) Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (…)"; Charter of Fundamental Rights of the European Union (2000/C 364/01) (Charter).

100 ***Digital Rights Ireland***, para 46 (with further references). In this case (supra, note 62), the retention on the basis of the Directive 2006/24/EC was found appropriate for fighting against serious crime (***Digital Rights Ireland***, para 49). Moreover, after stating that the existence of alternatives (like anonymous communication that could be deemed less harmful) did not affect appropriateness, the CJEU stressed that the retention could not be justified by the objective pursued, despite importance of this objective (***Digital Rights Ireland***, paras 50-51). Citing ***IPI***, which in turn referred to ***Satakunnan Markkinapörssi and Satamedia*** and ***Volker und Markus Schecke and Eifert***, the CJEU addressed proportionality in the strict sense. After highlighting the need for precise safeguards on the basis of ***Marper*** (***Digital Rights Ireland***, paras 54 and 55), the CJEU found that the interference was not limited to what was strictly necessary, since the Directive, among (many) others, affected anyone in a generalised manner and did not provide for adequate safeguards against abuse or misuse (***Digital Rights Ireland***, paras 56-59, 66-67). See: Case C-473/12 ***Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*** [2014] OJ C9/13 (***IPI***), para 39; Case C-73/07 ***Satakunnan Markkinapörssi and Satamedia*** [2008] ECR I-9831 (***Satakunnan Markkinapörssi and Satamedia***); Joined Cases C-92/09 and C-93/09 ***Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*** [2010] ECR I-11063 (***Volker und Markus Schecke and Eifert***).

To summarise, the matching (in the light of ***Breyer***) can be pictured as follows (Table 1):

Table 1: Proportionality lessons by the German regime, the EU doctrine, the CJEU and the ECtHR, in the light of Breyer

German regime[101]	EU doctrine	CJEU	ECtHR	Breyer
X	X	X	pressing social need[102]	pressing social need[103]
X	X	X	relevant and sufficient reasons justifying interference[104]	X
suitability	suitability	suitability / appropriateness[105]	suitability (to address the pressing social need)[106]	suitability[107]
necessity	necessity / alternatives	alternatives (if any)[108]	X	X
proportionality in the narrow sense	proportionality in the strict/narrow sense	proportionality in the strict/narrow sense, including: - balancing of goals/ rights against individual rights; and/or - assessment of whether the measure at issue exceeded what was necessary to achieve aim pursued (sometimes also looking for safeguards)[109]	proportionality of interference to aim pursued,[110] including: - balancing of public/private interests[111] - looking for safeguards[112] - looking for review possibilities[113]	proportionality of interference to aim pursued: - seriousness of national measure (gravity of interference)[114] - balancing of means/end (in the light of safeguards[115] and review mechanism)[116]

101 As analysed above, the notion of proportionality has its roots in the German legal regime. It was introduced in policing contexts to challenge measures disproportionate to the legitimate aim pursued by the authorities. Although crucial elements of this German version, such as the legitimate aim pursued, are mirrored in law and case law of the European Union and the Council of Europe, the concept of proportionality can have different meanings (and elements) when applied to different legal frameworks. See among others: Paul Craig and Gráinne de Búrca, ***EU Law*** (supra, note 85) 551; Robert Schütze, ***An Introduction to E***uropean Law (supra, note 86) 204-205. For an analysis of the reasoning of the German Federal Constitutional Court in balancing cases, see: Niels Petersen, 'Alexy and the "German" Model of Proportionality: Why the Theory of Constitutional Rights Does Not Provide a Representative Reconstruction of the Proportionality Test' (2020) 21 German Law Journal 163, 168-172.

102 See for example: ***Breyer***, para 88.

103 Breyer, para 88 ("(…) the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, upholding public safety and the protection of citizens constitute "pressing social needs"").

104 See for instance: ***Marper***, para 101; ***Segerstedt-Wiber***g, para 88.

105 See for example: ***Volker und Markus Schecke and Eifert***, paras 74-75; Sch***warz***, para 41; ***Digital Rights Ireland***, para 49.

106 See for example: Breyer, para 90.

107 To ***Breyer***, storage was the ***suitable*** response addressing the pressing social needs (of the fight against crime and the protection of citizens): first, telecommunications-related technology was deemed an important investigative tool to fight against crime (***Breyer***, para 88); second, storage (as the government had claimed) was an effective measure to aid the fight against crime (***Breyer***, paras 89-90); and, third, lack of consensus amid states broadened the margin of authorities to choose the suitable answer to technological changes (Breyer, paras 58, 90).

108 See for example: ***Volker und Markus Schecke and Eifert***, para 86; ***Schwarz***, para 46; ***Digital Rights Irelan***d, para 50.

109 See for example: ***Volker und Markus Schecke and Eifert***, para 86 (after balancing transparency-related goals and rights against the right to privacy and the protection of personal data, the Court found that the interference at issue had exceeded the limits imposed by the principle of proportionality); ***Schwarz***, para 63 (it was found that the measure had not gone beyond what was necessary to achieve the goal pursued; the Court found guarantees against abuse and misuse of data); Digital Rights Ireland, paras 56ff (the CJEU found that the measure was not limited to what was strictly necessary, since the Directive 2006/24/EC did not provide for adequate safeguards against abuse or misuse).

110 See for example: ***Breyer***, para 88.

111 See for example: ***Breyer***, paras 91ff.

112 See for example: ***Breyer***, paras 96-101.

113 See for example: ***Breyer***, paras 102-107.

114 In ***Breyer***, the interference caused by the national measure (storage) in question was deemed "of a rather limited nature" (***Breyer***, para 95).

115 On storage (under section 111), it was the "technical" safeguards, the "not inappropriate" duration and the limitation of the amounts of data to what was necessary for the subscriber's identification (***Breyer***, para 96). On access and use, it was section 112's exhaustive list of law enforcement-related authorities empowered to access data stored (***Breyer***, para 98), as well as section 113's detailedness resulting in foreseeability as to which authorities might request information stored (***Breyer***, para 99). Overall, it was the "double door" notion protecting against abuses of data stored, but also limitations of data to the necessary amounts and their subjection to delete-rules (***Breyer***, para 100).

116 The review-threshold was met by: the responsibility of the retrieving agency regarding legality of requests, in combination with competence of the Federal Network Agency with regard to admissibility of transmissions (***Breyer***, para 104); record-keeping/documentation and overall supervision of retrievals by the data protection authorities ensuring appeal-opportunities (***Breyer***, para 105); and more general rules in national law giving further opportunities to challenge retrievals (***Breyer***, para 106). These contest-opportunities made lack of notification and opacity of retrievals "privacy-compliant" (not violate Article 8 of the ECHR; ***Breyer***, para 107). To the above mechanism, ***Breyer*** added lack of consensus amid states enlarging the margin (***Breyer***, para 108).

2.5 A closer look at the Breyer necessity test

The table and analysis ***above*** suggest two things: firstly, there is no standard formula for the proportionality test in Europe; secondly, the ECtHR refuses to embrace one standard of scrutiny of proportionality or necessity. The higher the number of elements involved, the stricter the scrutiny that the ECtHR wishes to engage in.[117] If fewer elements are included, all that remains is a simple balancing exercise allowing only some sort of low-level scrutiny.

Breyer is an example of this latter scenario: intrusiveness of a rather limited nature, in conjunction with highly important goals (such public safety and crime prevention), allow for the examination of fewer proportionality-elements. This is predictable; not only in light of the above-cited surveillance case law, but also, and more importantly, given the aforementioned margin-considerations.[118]

117 We recall that the possible elements of the Strasbourg's necessity test can be "pressing social need" (not always mentioned by the Court), "sufficient and relevant reasons" (only applied when testing is stricter), "least harmful means" (very seldom used) and proportionality of the measure to the legitimate aim pursued. The last element serves as a baseline of the Strasbourg proportionality test that –whenever the Court finds it appropriate– is complemented with elements, such as "pressing social need" and "relevant and sufficient reasons" and, rarely, with the "least harmful means".

118 As noted above, interference-level and goal pursued can affect the margin of national authorities to introduce privacy-threating measures; the margin can in turn affect proportionality. In ***Breyer***, the (alleged) goal of striking down sophisticated crime (***Breyer***, paras 88-90), accompanied by an (allegedly) low-level interference (***Breyer***, paras 91-95), can (according to the Court) justify a broader margin and, therefore (and according to the above case law-analysis), allow for a looser proportionality test. The ECtHR refers to the margin in three instances: when recognising it; when applying it; and when concluding (reminding it). First, the Court accepts that the margin goes hand in hand with European supervision and it acknowledges that the scope of the margin is dependent upon several factors, including the aforementioned interference-level and goal pursued, as well as the consensus among states (***Breyer***, paras 79-80). Second, relying on a comparative analysis demonstrating no absolute agreement amid thirty-four states surveyed and some variations regarding the details, the Court recognises there is a wide margin of appreciation that renders storage via telecommunications technologies a suitable response to the detected pressing social need (***Breyer***, para 90). Last, the Court reminds lack of consensus in its conclusion to support the proportionality-related findings: the German authorities had a wide margin that they had not overstepped (***Breyer***, para 108). It is noted that, according to the comparative analysis, fifteen out of thirty-four States surveyed require storing of subscriber data. Despite variations regarding duration, purposes and procedural safeguards, most of the States provide for a list of authorities empowered to access subscriber data stored, restrict storage-purposes to fighting against crime or the prevention of threats to public order and demand that particular guarantees be met prior to access (like order by a court or public prosecutor). A minority requires notification of subscribers in case of access by authorities (***Breyer***, para 58).

The result is, as said, a looser proportionality test that lacks, among others, the examination of relevant and sufficient reasons. Skipping the question of whether there are relevant and sufficient reasons cited by the national authorities to justify storage of subscriber data would be absolutely understandable, were the goal of storage truly crime prevention and were the interference truly limited. But is it? We doubt it. So does Judge Ranzoni.

Judge Ranzoni in his dissenting to ***Breyer*** stresses that the case at hand "is not confined to measures concerning the fight against terrorism or other similar serious crimes, and nor is it limited to issues of national security"[119] and further argues that the storage of subscriber data is aimed at creating a "comprehensive register of all users of mobile communications".[120]

This development with regard to subscriber data fits well with the tendency to establish in all societal spheres population-wide databases of information for the purpose of identification, rather than control –control being the goal of old-school surveillance.[121] A wide array of services, from e-government[122] to e-banking,[123] are, or are planned to be, delivered through e-identification of the receiver of the service; that is, everyone. Such an indiscriminate identification-goal, going beyond or disregarding control (such as profiling) and whereabouts (like, location data), is to be achieved through the processing of non-highly intrusive data, such as subscriber data.[124] It is disappointing that ***Breyer*** neither sees nor addresses this identity-based surveillance. Perhaps in the future, the Court will have to answer questions about proportionality-, necessity- or human rights-compliance of these identity-based surveillance tools; straight questions that will be submitted by innocent citizens, like the Breyers.[125]

119 ***Breyer***, Dissenting Opinion of Judge Ranzoni, para 3.

120 ***Breyer***, Dissenting Opinion of Judge Ranzoni, para 7. Amendments to section 111 addressing the ever-growing phenomenon of registration of false data can support Judge Ranzoni's view (after the 2016 amendments to section 111, subscribers must provide proof of their identity). See: supra, note 1; ***Breyer***, para 28; Dissenting Opinion of Judge Ranzoni, para 7.

121 See for instance: David Garland, ***The Culture of Control: Crime and Social Order in Contemporary Society*** (University of Chicago Press 2001).

122 European Commission, 'e-Identification' <https://ec.europa.eu/digital-single-market/en/e-identification> accessed 17 May 2020.

123 CEF Digital, 'The potential of electronic identification under eIDAS in the banking sector' (CEF Digital, 15 March 2019) <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/03/15/The+potential+of+electronic+identification+under+eIDAS+in+the+banking+sector> accessed 17 May 2020.

124 In this regard, Rommetveit argues that, over the past decades, the key-goal has been the establishment of identities and interoperability amid databases; but the problem has been the absence of databases. The author discusses how face recognition (or other biometric-implementations) can, when accepted by educated citizens, be deployed by governments to fulfil identification- and interoperability-related goals. Kjetil Rommetveit, 'Introducing Biometrics in the European Union: Practice and Imagination' in Ana Delgado (ed), ***Technoscience and Citizenship: Ethics and Governance in the Digital Society*** (Springer 2016) 113.

125 Our intuition is supported by emerging identity-surveillance mechanisms that are increasingly embraced and adding criminal dimensions to everyday life. See for example live or retrospective face recognition: ICO, ***ICO Investigation into How the Police Use Facial Recognition Technology in Public Places*** (ICO, 31 October 2019) <https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf> accessed 17 May 2020; Home Office, 'Fact Sheet on live facial recognition used by police' (GOV.UK, 4 September 2019) <homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/> accessed 17 May 2020. See also discussions on Google and Apple's tracing-response to the Coronavirus outbreak: Tech Crunch, 'Apple and Google are launching a joint COVID-19 tracing tool for iOS and Android' (***Tech Crunch***, 10 April 2020) <https://techcrunch.com/2020/04/10/apple-and-google-are-launching-a-joint-covid-19-tracing-tool/> accessed 17 May 2020; on Alicem that assists the French government in delivering services via face recognition: Ministère de l'Intérieur, 'Alicem, la première solution d'identité numérique régalienne sécurisée' (Ministère de l'Intérieur, 19 December 2019) <https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee> accessed 17 May 2020; The Telegraph. 'France to become first EU country to use nationwide facial recognition ID app' (***The Telegraph***, 3 October 2019) <https://www.telegraph.co.uk/news/2019/10/03/france-become-first-eu-country-use-nationwide-facial-recognition/> accessed 17 May 2020; on the UK's strategies involving identity-gathering/verification with the support of the private sector: GOV.UK, 'Guidance GOV.UK Verify' (GOV.UK, 25 March 2020) <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify> accessed 17 May 2020.

If our intuition is true, we hope that the Court will take into due consideration any additional goal pursued (especially, in relation to identification), as well as the interference-level (potentially interference with the data of entire populations). These two elements, taken seriously, would perhaps affect the margin of appreciation and should, in our view, call for a stricter version of the proportionality test. It would then be desirable that the Court adds more elements to its proportionality testing, such as "sufficient and relevant" reasons, to tackle future ***Breyer***-like cases. As revealed by earlier case law, the relevant and sufficient reasons justifying retention of data could consist of the enlargement of databases of ***known*** individuals that contributes to crime prevention.[126] This propensity to enlarge databases of the ***known*** is accompanied by the tendency to reduce the pool of the ***unknown*** –through, for example, forensic DNA phenotyping that tells how the unknown suspect could look like and, hence, (allegedly) helps limit the pool of suspects to, for instance, "man, tall, blue-eyed, from Europe".[127] If we are moving toward registers of knowns and disappearance of the unknowns, toward the "disappearance of disappearance"[128] where anonymity is a myth, it would be preferable for the Court to accept the challenge and opt for stricter versions of the proportionality test.[129]

3. Conclusion: Stricter Proportionality Test for Identity-Based Surveillance?

The previous discussion demonstrates how blurring Article 8 ECHR-requirements such as legality and necessity can affect the quality of the Court's reasoning, the legality test and the proportionality assessment. Our analysis of the testing by the Court of the legality requirement, its rise and its fall, reveals a tendency to relax scrutiny when interference is considered to be of a limited nature. In these cases, the Court tends to skip crucial checks. ***Breyer*** illustrates our point: it disregards collection and storage and focuses on access, use and ex post regulation.[130] Of course, we welcome review of German law with regard to access, use and ex post control. Precautions on access and, in general, on subsequent uses of data stored (like sharing or disclosing) must be in place. However, similar or, perhaps, even more stringent guarantees must exist at the initial stage of collection/storage as well. Silence on collecting and storing data, on what constitutes the interference the Court is dealing with, is troublesome. Privacy can be harmed when data are taken. After-the-harm measures are not the ideal cure for this.

126 ***Marper***, para 117.

127 A brief, yet comprehensive analysis of DNA phenotyping in: VISAGE, 'The VISAGE Consortium' (VISAGE) <http://www.visage-h2020.eu/> accessed 17 May 2020.

128 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51(4) British Journal of Sociology 605, 619.

129 In addition to our claim that the proportionality test should be stricter (provided the goal of storage were deemed to be identification), and considering the particularities of ***Breyer***, and in the light of the ECtHR's authority to invoke the uninvoked (like sections 112 and 113), as well as identify additional purposes pursued by storage (such as identification), it could be fairly argued that, in this case, the ECtHR could have used Article 18 of the ECHR, despite it not being invoked, to more accurately assess proportionality. Under Article 18, the "restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed". In ***Breyer***, identification could have been deemed an identifiable ulterior purpose nowhere prescribed in the ECHR. Then, the storage of subscriber data could have been considered as pursuing an ulterior purpose, contrary to Article 18 of the ECHR. This could affect the proportionality assessment of the Court and reach a different outcome: violation of the right to privacy. Such approach and outcome might better fit high levels of interference with the rights of the affectable (very likely entire) population, as well as the goal of identification of citizens, rather than criminals. In this regard, it is noted that the ***Marper***-Court used Article 6 of the ECHR that had never been invoked by the applicants to better assess necessity of interference (***Marper***, para 122). For a recent authority on the interpretation of Article 18 of the ECHR, see: ***Kavala v Turkey*** Application no 28749/18 (ECtHR, 10 December 2019), paras 215-232 (with further references).

130 As noted above, after a brief examination limited to the duration and scope of storage (***Breyer***, para 96), the Court assessed safeguards with regard to access and use under sections 112 and 113.

For a proper testing of proportionality and necessity, one has to ask a very basic question: ***what is the interference caused by a certain measure or legal instrument and what is the goal***? These are questions that, after reading ***Breyer***, still cannot be answered with certainty. Identifying everyone can, without any doubt, help authorities fight crime; for they know who to look for. But then everyone becomes suspected and no one remains anonymous. How is it possible that the ***Breyer***-judgment does not take seriously, but rather easily skips the freedom of expression-discussion? Especially when it is the very taking of the data, the storage that the applicants invoke and that the Court avoids to analytically assess throughout the whole judgment, that which causes identifiability and, thus, kills anonymity?[131]

The central message of ***Breyer*** seems to be "do not worry too much about identification surveillance, since there are guarantees with regard to use and ex post controls in the German Telecommunications Act, complemented by the guarantees in the German Data Protection Act and the supervision by the German data protection authority". Are we reassured? Data protection laws seem to have eaten everything. We make laws to regulate humans, their matters and affairs; and every human is by her nature inevitably connected with data. So, every attempt to regulate can trigger data privacy laws, but is this the proper approach to regulate?[132]

131 ***Breyer***, paras 60-63, in particular paras 61-62 ("(…) while the Court is mindful of the circumstances of the data storage at issue and its proximity to telephone communications and the right to correspondence, it considers that the key aspect of the applicants' complaint is the storage of their personal data and not any particular interference with their correspondence nor with their freedom of expression (…) The Court is therefore not called in the present case to decide if and to what extent Article 10 of the Convention maybe be considered as guaranteeing a right for users of telecommunication services to anonymity (…) and how this right would have to be balanced against others imperatives (…)").

132 For instance, when we regulate alcohol-consumption at work via introducing alcohol-checks at the workplace, it may be wiser to consider, first, labour law (do we want these tests? are they lawful under labour law?) and, then, any data/privacy implications (once unlawful under labour law, they would be unlawful on the basis of the unlawfulness of processing). Similarly, when regulating communications through demanding people to prove who they are, it may be wiser to consider, first, telecommunications law (do we want such proof? is it lawful to ask everyone to prove their identity under telecommunications law?) and, then, data/privacy concerns. The requirement of proving identity conflicts, first of all, with the aim of safeguarding "the interests of users in the fields of telecommunications and radiocommunications" and maintaining "telecommunications secrecy". This appears as the primary goal of telecommunications and frequency regulation in the German Telecommunications Act (section 2(2)(1)); and it definitely includes the right "to receive and impart information and ideas without interference by public authority and regardless of frontiers" (ECHR, art 10(1)). Then, it would be desirable to be a little more "mindful of the circumstances of the data storage (…) and its proximity to telephone communications" (***Breyer***, para 61), consider with appropriate care and diligence "any particular interference with (…) freedom of expression" (***Breyer***, para 61) and, if necessary, feel a duty to "decide if and to what extent Article 10 of the Convention maybe be considered as guaranteeing a right for users of telecommunication services to anonymity (…) and how this right would have to be balanced" (***Breyer***, para 62) against other imperatives. .

ANNEX[133]

Section 111 of the Telecommunications Act:

"(…) (1) Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties or other identifiers of the respective allocation, is, for the information procedures under sections 112 and 113, to collect, prior to activation, and store without undue delay:

1. The telephone numbers and other identifiers of the respective allocation;
2. The name and address of the allocation holder;
3. The date of birth in the case of natural persons;
4. In the case of fixed lines, additionally the address for the line;
5. In cases in which a mobile-communication end device is made available together with the mobile-communication allocation, also the device number of the said device, as well as;
6. The effective date of the contract.

Even if such data are not necessary for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers. … A person with obligations under sentence 1 or sentence 3 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations under sentence 1 is subsequently to collect and store data not yet recorded if collecting the data is possible with no special effort. The manner in which data for the information-retrieval procedure provided for under section 113 are stored is optional.

(2) Where the service provider in accordance with subsection (1) sentence 1 or sentence 3 operates in conjunction with a sales partner, such a partner shall collect data according to subsection (1) sentence 1 and 3 under the pre-requisites set out therein and shall transmit to the service provider, without undue delay, these and other data collected under section 95; subsection (1) sentence 2 applies accordingly. Sentence 1 also applies to data relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.

(3) Data within the meaning of subsection (1) sentence 1 or sentence 3 need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1) sentence 4.

(4) The data are to be erased upon expiry of the calendar year following the year in which the contractual relationship ended (…)".

133 This ANNEX contains relevant parts of sections 111, 112 and 113 of the German Telecommunications Act as mentioned in: ***Breyer***, paras 27, 29 and 31.

Section 112 of the Telecommunications Act:

"(…) (1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111(1) sentences 1, 3, and 4, and subsection (2) in customer data files …. The obligated person shall ensure that:
1. the Federal Network Agency is enabled, at all times, to retrieve data from customer data files by way of automation within Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.
The obligated person and his agent are to ensure by technical and organisational measures that no retrievals can come to their notice. The Federal Network Agency may retrieve data from customer databases only to the extent that knowledge of the data is necessary:
1. in order to prosecute administrative offences under the present Act or under the Unfair Competition Act [*Gesetz gegen den unlauteren Wettbewerb*];
2. in order to process requests for information lodged by the bodies set out in subsection (2).
The requesting body shall verify without undue delay to what extent it needs the data transmitted in response to its request and shall erase any data it does not need without undue delay; this shall also apply to the Federal Network Agency regarding the retrieval of data in accordance with sentence 7 no. 1.

(2) Information from the customer data files according to subsection (1) shall be provided to:
1. the courts and criminal prosecution authorities;
2. Federal and ***Land*** law-enforcement authorities for purposes of averting danger;
3. the Customs Criminal Investigations Office [*Zollkriminalamt*] and customs investigation offices [*Zollfahndungsämter*] for criminal proceedings and the Customs Criminal Investigations Office for the preparation and execution of measures under section 23a of the Customs Investigation Service Act [*Zollfahndungsdienstgesetz*];
4. Federal and ***Land*** offices for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office, and the Federal Intelligence Service;
5. the emergency service centres under section 108 and the service centre for the maritime mobile emergency number "124 124";
6. the Federal Financial Supervisory Authority; and
7. the authorities of the customs administration for the purposes listed in section 2(1) of the Undeclared Work Act [*Schwarzarbeitsbekämpfungsgesetz*] via central enquiries offices.
as stipulated in subsection (4), at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures. …

(4) At the request of the authorities referred to in subsection (2), the Federal Network Agency is to retrieve and transmit to the requesting authority the relevant data sets from the customer data files in accordance with subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with:
1. the Federal Network Agency, in the cases governed by subsection (1) sentence 7 no. 1; and
2. the bodies set out in subsection (2), in the cases of subsection (1) sentence 7 no. 2.
For purposes of data-protection supervision by the competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, information clearly identifying the person retrieving the data, as well as the requesting authority, its reference number, and information clearly identifying the person requesting the data. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year (…)".

Section 113 of the Telecommunications Act:

"(…) (1) Any person commercially providing or assisting in providing telecommunications services may use, subject to the stipulations of subsection (2), the data collected under sections 95 and 111 in accordance with this provision of the Law in order to fulfil its obligations to provide information to the bodies listed in paragraph 3. …

(2) The information may be provided only inasmuch as one of the bodies set out in paragraph 3 has requested that this be done, in text form, in an individual case in order to prosecute criminal or administrative offences, in order to avert danger to public safety or order, and in order to discharge the legal functions of the bodies set out in subsection (3) no. 3, citing a provision of the law that allows it to so collect the data referenced in subsection (1); no data pursuant to subsection (1) may be transmitted to any other public or non-public bodies. In the case of imminent danger, the information may be provided also if the request is made in a form other than text form. In such an event, the request is to be confirmed subsequently in text form; this shall be done without undue delay. Responsibility for the admissibility of the request for information lies with the bodies set out in subsection (3).

(3) The following are "bodies" in the sense of subsection (1):
1. The authorities responsible for prosecuting criminal or administrative offences;
2. The authorities responsible for preventing threats to public security or to public order;
3. Federal and Land offices for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office, and the Federal Intelligence Service.

(4) A person commercially providing or assisting in providing telecommunications services is to transmit the data to be provided pursuant to a request completely and without undue delay. The parties obligated to provide information are to keep confidential requests for information and the provision of information both vis-à-vis the party/parties affected and vis-à-vis third parties (…)".

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

N°26 European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law (September 2020) by Angela Aguinaldo and Paul De Hert (16 pages)

N°27 Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership (June 2021) by Paul De Hert and Georgios Bouchagiar (24 pages)

N°28 Adding and removing elements of the proportionality and necessity test to achieve desired outcomes. Breyer and the necessity to end anonymity of cell phone users (September 2021) by Paul De Hert and Georgios Bouchagiar (26 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Editorial Board: Paul De Hert and Christopher Kuner

Contact: info@brusselsprivacyhub.eu