CMS
law·tax·future

European Court of Human Rights
Council of Europe
F-67075 STRASBOURG – CEDEX

FRANCE

Via fax in advance: + 33 (0)3 88 41 27 30

App No. 81996/17 24.06.2021

In the matter

Rechtsanwalt Niko Härting vs. Federal Republic of Germany

– having received the letter of 4 June 2021 – the following comments are submitted on behalf of the Council of Bars and Law Societies of Europe (CCBE) to the European Court of Human Rights, Third Section.

Introduction

1. These observations are submitted on behalf of the Council of Bars and Law Societies of Europe ("the CCBE"), with particular support from Iain Mitchell, QC, of the Scottish and English Bars, and Vice Chair of the CCBE's surveillance committee, in response to the invitation by the Vice-President of the Third Section of the Court given by letters dates 15th March and 4th June 2021. The submission focuses exclusively on the particular interests of the CCBE in the case before the Court.
2. The CCBE is the European organisation representing over one million lawyers in Europe. Its purpose is, in particular, to represent the European national bars and law societies in all matters of common interest relating to the practice of the legal profession, respect for the rule of law and the proper administration of justice, as well as representing those bars and law societies in relation to legal developments at both European and international levels.

3. The CCBE also aims to act as an advisory and intermediary body amongst its members, whether full members, associates or observers, and between its members and the institutions of the European Union, the European Economic Area and the Council of Europe respectively in all cross-border matters of common interest, but also to ensure respect for the rule of law, human rights and the protection of fundamental rights and freedoms, including the right of access to justice and the protection of citizens, as well as the protection of the democratic values intimately linked to the exercise of these rights. The CCBE has intervened in numerous landmark cases also relating to Internet-related human rights and media freedoms, including before this Court in case of *Morice v. France* (App. No. 29369/10), *Michaud v. France* (App. No. 29369/10), *Mor v. France* (App. No. 28198/09), and *Association Confraternelle de la Presse Judiciare v. France* (App. No. 49526/15) (App. Nos. are not repeated hereafter.)

4. A particular interest of the CCBE as an organisation representing European lawyers is to defend actively the rule of law, and, in this context, to seek to ensure the protection of legal professional privilege (hereinafter jointly referred to as "**LPP**") and professional secrecy. It seeks to defend access to justice, and to promote respect for the law, including the protection of human rights. This includes advocating for effective legal protections of fundamental rights. In the present matter, several of these issues are at stake, and lawyers and citizens in all of the 45 countries represented by the CCBE are affected. This Application raises issues of considerable public importance which touch on the freedoms of residents, within the Council of Europe States and beyond, whose international telecommunications are or may be monitored. In these written comments, the CCBE restricts itself to addressing only the general principles applicable to the interaction between mass surveillance regimes and the protection of fundamental rights, without addressing the particular facts or merits of the Court case.

Development of the law concerning mass surveillance in the light of technological change

5. The European Convention on Human Rights is a living instrument, the interpretation and application of which requires constantly to evolve in order to respond to changes in society. This is particularly the case in relation to the tension between the protections accorded by Article 8 of the Convention (Articles thereafter refer to the Convention if not stated otherwise) and the increasingly intrusive techniques of mass surveillance employed by state actors. As the ability of States to carry out interferences by modern technology has increased exponentially in recent years due to huge advances in computing power and the ever more sophisticated surveillance measures which that increase enables, so, too, the perceived necessity of deploying those measures has become more pressing with genuine concerns on the part of States to protect society from external threats. However, there is a clamant need that there should be struck a balance between what can, technologically be done, and what it is proportionate to do – just how far the state can properly and proportionately go in undertaking measures which intrude upon the privacy of its citizens. In this regard, the Court will recall that in the case of S. and Marper v The United Kingdom (Apps Nos. 30562/04 and 30566/04) the UK Government sought to justify the indefinite retention of a database containing, inter alia, DNA samples, was justified as being "of inestimable value in the fight against crime and terrorism."(§91). Nevertheless, the Grand Chamber, whilst accepting the importance of such information in the detection of crime (§106), observed (at §112) that "the protection afforded by Article 8 would be unacceptably

weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests." This is an issue of proportionality.

6. The use of such techniques may also engage the question of whether and to what extent the measures complained of are *in accordance with the law*. The Court will recall that the Grand Chamber in *S. and Marper* at §99 reiterated that:

7. "it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness".

8. These remarks are especially pertinent in any case which may involve mass surveillance of electronically transmitted communications.

9. The first relevant case in which the court engaged with the issue of mass surveillance, in particular, was *Klass and others v. Germany* (App. No. 5029/721), which concerned a lawyer who sought a determination concerning the German surveillance regime. It was a characteristic of that regime that he was not informed whether he was subject to surveillance and was therefore unable to establish an infringement of his own individual rights. However, the court determined that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures." (§24). On the substantive question, the Court found that there had not been any violation of his Convention rights.

10. From this *starting* point, the jurisprudence of the Court has developed substantially over the intervening period of in excess of 40 years, but, until recently, has not fully kept up with the explosive development in the technology of surveillance. The revelations concerning surveillance in the context of the NSA in the USA and its counterparts all over the world have shown that secret surveillance can affect everyone, and since it is secret, special legal mechanisms must exist to protect the individual. It was in that context that the Court took advantage of the opportunity in the recent cases of *Big Brother Watch and Others v. the United Kingdom* (App. Nos. 58170/13, 62322/14 and 24969/15) and *Centrum för rättvisa v. Sweden* (App. No. 35252/08) to restate the law governing the protection of Article 8 in the context of mass surveillance activities. These decisions represent a paradigm shift in the legal regime. Previous cases may sometimes provide useful context, but the present intervention takes as its point of departure the guidance given by the Grand Chamber in the aforementioned cases. In the following, these cases will be put into context in more detail.

Present state of the Law regarding mass surveillance

11. In *Big Brother Watch and Others v. the United Kingdom* the Grand Chamber recognised that, owing to the proliferation of threats that States faced from networks of international actors, who use the Internet for communication in pursuit of their harmful objectives, member States of the Convention have a wide discretion ("margin of appreciation") in deciding what kind of surveillance scheme may be necessary to protect national security. Accordingly, the Court stated that a decision to operate a bulk interception regime did not of itself violate Article 8. However, having considered the specific features of the UK bulk interception regime, the Grand Chamber found that there had been, in this case, a violation of Article 8.

12. The Court considered that, in view of the changing nature of modern communications technology, its approach towards surveillance regimes needed to be adapted to take into account the specific features of a bulk interception regime which creates both an inherent risk of abuse and a legitimate need for secrecy. In this context the Grand Chamber identified the need to ensure what it described as "end to end safeguards". This requires an assessment of both necessity and proportionality at each of the stages of (a) at the outset; (b) whilst surveillance is being undertaken and (c) the availability of *ex post facto* review (§350). In addressing this issue, the Court formulated the following eight aspects which the domestic legal framework has to clearly define: (1) the grounds on which bulk interception may be authorised; (2) the circumstances in which an individual's communications may be intercepted; (3) the procedure to be followed for granting authorisation; (4) the procedures to be followed for selecting, examining and using intercept material; (5) the precautions to be taken when communicating the material to other parties; (6) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; (7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; (8) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance (§361).

13. Following from the above, a domestic regime that lacks specific safeguards such as: (1) the absence of a clear rule on the destruction of intercepted material – even if it only concerns material that does not contain personal data; (2) the absence of a requirement in the relevant legislation that individuals' privacy interests be taken into account when deciding to transfer intelligence material to foreign partners; and (3) the absence of effective *ex post facto* review, will lead to a violation of Article 8 (*Centrum för rättvisa v. Sweden* §§369-374).

14. Further, taking into account the (secret) nature of bulk surveillance, the scale of its application and the risk of an abuse of power, according to the Grand Chamber the following key criteria need to be fulfilled in order for a bulk surveillance regime to be compliant with Convention standards (see *Big Brother Watch and Others v. the United Kingdom §§*340-360 and *Centrum för rättvisa v. Sweden* §§369-377):

    - "**End to end safeguards**", meaning that, at the domestic level, an assessment should be made at each stage of the process – before, during and after the bulk interception measures – of the necessity and proportionality of the measures being taken;

- bulk interception should be subject to **authorisation** (identifying at least the types or categories of selectors to be used) **by an independent body** at the outset, when the object and scope of the operation is being defined, and the independent body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted; "independent body" meaning a body which is not only independent of the institution carrying out the bulk surveillance, but of the executive as a whole;
- the **use of every selector used must be justified** with regard to the principles of necessity and proportionality by the intelligence services, and that justification should be scrupulously recorded and subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles;
- each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to **supervision by an independent authority**, and that supervision should be sufficiently robust to keep the interference to what is "necessary in a democratic society". In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected.
- in order to facilitate the supervision, **detailed records should be kept** by the intelligence services at each stage of the process;
- an **effective remedy** should be available to anyone who suspects that his or her communications are or have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime; for this purpose there either needs to be a subsequent notification of the concerned individuals about the surveillance measures taken, or the system of domestic remedies must permit any person who suspects that his or her communications are being or have been intercepted to apply to the courts.

15. In addition, the transfer of intercepted material to other parties is subject to several restrictions specified by the Grand Chamber (see *Big Brother Watch and Others v. the United Kingdom* §362):

- the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner;
- the circumstances in which such a transfer may take place must be set out clearly in domestic law;
- the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure;

- heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred;
- the transfer of material to foreign intelligence partners should also be subject to independent control.

16. The Grand Chamber further found that, in the context of bulk surveillance, the retention of communications data should be analysed by reference to the same safeguards that apply to content (see *Big Brother Watch and Others v. the United Kingdom* §§352-357).

How the questions relate to any given Bulk Surveillance Regime

17. The above-mentioned cases show that the European Court of Human Rights subjects to particular scrutiny national legal regimes of bulk surveillance. It is no longer sufficient for a state merely to invoke its wide margin of appreciation. Rather, the above-mentioned specific criteria must be met. This has particular significance when also taking into account the "chilling effect" of monitoring. This enhanced scrutiny applies not only to any kind of monitoring of personal data, but also to the monitoring of any form of communication between sender and recipient, all of which fall within the scope of the protection afforded by Article 8. Since surveillance regimes may differ from state to state, the outcomes of the scrutiny may differ from state to state, depending on the specifics of the regime under scrutiny, but, looking back at *Big Brother Watch*, *Centrum för rättvisa* and the previous cases, certain commonalities emerge: They focus on the principles of necessity and of proportionality, on the need for documentation and for effective legal protection.

18. The CCBE welcomes that the Court has further developed and restated the criteria for judging the legality of bulk surveillance regimes and sees this as an important step effectively to secure a sufficiently high level of protection of human rights in the member States: the more intensive the interference, the more protection must exist *ab-ante*, the more the supervision and control which must exist while the surveillance measures are ongoing and the greater must be the procedural protection *ex post facto*. These principles also have a meaningful context in the classification of cases such as *Roman Zakharov v. Russia* (App. No. 47143/06) which focused on the availability and effectiveness of a remedy on a national level against arbitrariness and the risk of abuse inherent in any system of secret surveillance. The current criteria have expanded on this and include as an important element the supervision by an independent body and legal protection during the various procedural stages of surveillance.

Special Concerns related to LPP/Professional Secrecy

19. The need for such protections of Article 8 rights assumes heightened importance where the material which is subjected to mass surveillance includes communications between lawyers and clients. Such communications will normally be subject to obligations of LPP. LPP is a fundamental component of the rule of law. This receives particular recognition in terms of Article 6 which affirms a right which is absolute, and not qualified (see, for example, *Neimietz v Germany* (App. No. 13710/88)), especially at §37) but even seen through the lens of Article 8 (which is a qualified right) there is afforded strengthened protection to exchanges between lawyers and their clients, upon the basis that the maintenance of trust in the confidentiality of such communications is essential to the

fundamental role of lawyers in a democratic society and for the rule of law. The Court will recall that it articulated this principle of strengthened protection in the landmark case of *Michaud v. France* (at §§118 and 119). It follows from this that lawyers cannot carry out their essential task if they are unable to guarantee to their clients that their exchanges remain confidential. In the context of LPP "the notion of necessity implies that the interference corresponds to a social need and, in particular, that it is proportionate to the legitimate aim pursued" (see *Foxley v. UK* (App. No. 33274/96) §43 and *Pruteanu v. Romania* (App. No. 30181/05). Exceptionally, in *Michaud v. France,* the Court did not consider that there had been an infringement of Article 8. The case concerned the lawfulness, under the Convention of legislation imposing an obligation on lawyers to report suspicions of money laundering. The Court recognised (§§121 and 124), that where a lawyer is himself engaged in an illegal act, such as money laundering, communications regarding this act do not fall within the scope of LPP. The Court had regard to the importance of the obligation to report suspicions of money laundering (§123) and, in considering the imposing of the obligation to meet the test of proportionality, treated two factors as decisive: first, that the obligation to report suspicions of money laundering did not concern the core area of the lawyer's defence role which forms the basis of legal privilege (§§127 and 128) and, second, that lawyers were not required to transmit reports directly to a government institution (in that case the FIU) but, as appropriate, to the President of the Bar Council of the Conseil d'Etat and the Court of Cassation or to the Chairman of the Bar of which the lawyer is a member (§129). Bulk surveillance is carried out without the consent, and frequently without even the knowledge of surveillance subjects, including lawyers. There is no question of there arising an obligation on the part of a lawyer to report anything – surveillance is essentially involuntary. There is simply no mechanism to engage the safeguard of indirect reporting to the President of Bar, as that is not what surveillance is about. Further the infringement of Article 8 potentially affects every communication between lawyers and clients, and is overwhelmingly likely to lead to the interception of communications which do concern the core area of the lawyer's activities.

20. In light of the evolving jurisprudence of the Court, both in respect of LPP and in respect of the principles developed in *Big Brother Watch* and *Centrum för rättvisa,* the CCBE submits that it is of critical importance to the maintenance of the rule of law, of which LPP is an important component, that, in articulating further principles in the present or future cases, the Court should take advantage of the opportunity to consider whether there are in place in any mass surveillance regime, enhanced protections for legally privileged communications. Further, in assessing the Convention compliance of such regimes, the Court should consider whether, even if the regime in question does not infringe Article 8 in respect of "normal" correspondence, whether it nonetheless fails to afford to legally privileged communications the strengthened protection the necessity for which has been developed by the Court in its jurisprudence.

21. In particular, such strengthened protection of LPP should entail clearly articulated regulations dealing with the manner in which legally privileged communications fall to be treated in the context of bulk surveillance. Such regulations should ideally prevent privileged communication from being read at all (e.g. by technological means) or, if that should not be possible, there should be a guarantee that the communication upon being read (automatically or manually) is immediately destroyed and that none of its content nor

even the fact of its existence are stored in any way or are passed on to anyone. Independent supervision and an *ex post facto* review are necessary in order to guarantee that these rules are respected without exception. Severe penalties should apply in the event of infringement of these rules. Only with such strict rules will it be possible to prevent a lasting negative impact on the trust which is a crucial component in the relationship between lawyer and client. The erosion of that trust would result in a lasting negative impact on the rule of law.

22. A further issue to be considered is that, if the mass surveillance regime under review fails to provide the requisite protection to legally privileged communications, but otherwise sufficiently protects "ordinary" communications, the entire regime is therefore not Convention compliant. Logically, if no distinction is made within the regime between legally privileged communications and "ordinary" communications, this must inevitably be so. In the context of Article 8 there may, or may not, be scope for conducting a balancing exercise in considering the proportionality of the interference; but, in a future case, where Article 6 may be invoked, any infringement of LPP must necessarily invalidate the entire regime, given the unqualified nature of Article 6 rights.

The wider legal framework regarding surveillance

23. In the context of new surveillance technologies, bulk surveillance has led the Court, as set out above, to develop a restated framework for testing Convention compliance. The balancing of the perceived need for security against the protection of fundamental rights requires that interferences with Article 8 rights be fenced with "end-to-end safeguards". In the absence of such safeguards, the intrusions are unlikely to pass the test of proportionality. The safeguards need to be even stricter where the communications subject to surveillance are afforded special protection by the law. This may apply to journalists and other professions, but it certainly applies to legally privileged communications. The relevant domestic legal regime must provide sufficient safeguards and remedies, especially in cases where the surveillance in question *de facto* affects all mail traffic with foreign countries, and in cases where the selectors which have been chosen are unclear, ambiguous or opaque and are likely to affect almost every citizen.

24. The CCBE therefore warmly welcomes the direction of travel of the Court's jurisprudence as seen in its most recent decisions. The CCBE notes the emphasis on having clear rules for bulk intercept regimes in all member States of the Convention. Proper legal protection is essential in any bulk surveillance regime and the CCBE emphasises that any legal protection must involve supervision and control by an independent body, and must be effective, which is to say that it must be designed in such a way that the individual's rights are protected in a comprehensive and verifiable manner. To this end, the independent body judging the surveillance needs to be equipped with personnel, material and professional means to deal with bulk surveillance, regardless of whether someone is described as a "hit" or is notified (as to the latter see, for example, *Roman Zakharov v. Russia* (App. No. 47143/06)).

25. It is noteworthy that the Court of Justice of the European Union (ECJ) is developing a similar framework when judging privacy issues. In particular, in its judgement in the case *Privacy International* (C-623/17), the ECJ recognised, with respect to the Charter of Fundamental Rights of the European Union, "that the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the

right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter. Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistle-blowers" (§72). The ECJ concluded therefore "that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society" (§81). This judgment is in accord with the approach taken by the European Court of Human Rights to the chilling effects of mass surveillance measures which exceed the limits of what is strictly necessary, and, in developing its own jurisprudence, the Court, whilst acknowledging that mass surveillance is not *per se* unlawful (*Klass*), should follow the lead of the ECJ by subjecting any surveillance regime to particular scrutiny in relation to the test of necessity.

26. The Court may also wish to have regard to the decision of the European Court of Justice in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (C-311/18). In that case, the ECJ considered whether the EU-US Data Protection Shield afforded an adequate level of data protection in respect of personal data transferred thereunder to the United States. It found the level to be inadequate and invalidated the Data Shield. Of particular relevance to mass surveillance regimes was the observation by the ECJ (at §176) that the legislation in question "must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592 §§140-141 and the case law cited)". Of particular relevance are paragraphs 183 and 184:

> "183. It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target… to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O.12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data."
>
> "184. It follows therefore that neither Section 702 of the FISA, nor E.O.12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary."

27. Thus, the principal features rendering the Shield ineffective were the indiscriminate mass collection of data and the lack of effective remedies. As the Court considers cases in which it is called to assess the compatibility of mass surveillance regimes with Article 8, it should be mindful of the approach taken by the ECJ under the equivalent provisions in the EU Charter and seek to avoid a disconnect between the two fundamental rights regimes in Europe. In particular, it would be anomalous if European secret services could act in basically the same manner as the US surveillance authorities without breaching the law, while at the same time similar practices by the US authorities were found to be incompatible with the privacy rights of data subjects resident in the EU.

Conclusion

28. In summary, the rules generally applicable to the protection of Article 8 rights in the context of bulk surveillance have been undergoing a process of evolution, culminating in the landmark cases *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden*. Those rules now take into account the nature, scope and extent of the measures, the existence of proper controls and the availability of effective *ex post facto* remedies to persons subject to surveillance. They also serve to create a framework for surveillance which is as legally secure as possible, and which strengthens confidence in the rule of law.

29. However, these rules are ripe for further development to take account of the particular types of communication (notably legally privileged communications) which the jurisprudence of the Court has already found to be demanding of heightened protection at each of the three stages of control envisaged by the Court: at the outset, whilst surveillance is being undertaken and by way of effect *ex post facto* remedies.

30. The CCBE trusts that these comments will be helpful to the Court as it develops its jurisprudence further and that, in particular, the need for special protection of professional secrecy and legal professional privilege (LPP) will be taken account of in that development. In States governed by the rule of law, citizens are in need of protection against bulk surveillance, and the criteria developed by the Grand Chamber have, in the opinion of the CCBE, the potential to provide this protection, in particular if the Court decides to further develop these criteria in such a way that they also provide adequate protection for privileged communication.

i.V.

Dr. Sebastian Cording

Rechtsanwalt