Peyrot, Schlegel & Györffy
Rechtsanwälte

Zurich, 30 June 2023

Viktor Györffy
Rechtsanwalt
Beethovenstrasse 47
8002 Zürich
Telefon 044 240 20 55
Telefax 043 500 55 71
gyoerffy@psg-law.ch
www.psg-law.ch

Mr. Milan Blaško,
Section Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg cedex

Application No. 47351/18
G. and others v. Switzerland

Dear Mr. Registrar,

1. In the matter referred to above, I refer to your letter of 17 March 2023 in which you invite me to submit the points of disagreement regarding the Government's presentation and my observations in reply and requests for just satisfaction on behalf of the applicants, and to your letter of 4 April 2023 in which you invite me to submit to file written observations in reply to the third-party submission made by the Estonian Government.

2. Within the time allowed, I submit to you the following observations:

I. Subject of the dispute

3. The subject matter of the dispute is presented too narrowly by the government. Likewise, the government misjudges the appellants' protected interest in having all of their requests decided.

4. The government argues that a distinction must be made between administrative law and criminal law aspects concerning data retention. The transfer of stored metadata, the government states, concerns the aspects of the interception of telecommunications which were to be assigned to criminal proceedings. The metadata could therefore only have been transferred to the authorities on the basis of a surveillance order. In the

absence of a surveillance order, there is no sufficiently current interest to protect in the present case to rule on the applicants' request that the providers be ordered not to disclose the traffic and billing data concerning them to the Post and Telecommunications Surveillance Service (PTSS) or to other authorities or courts. According to the Government, it is justified that the national courts did not intervene in the applicants' request to order the providers not to disclose the traffic and billing data concerning them to the PTSS or to other authorities or courts.

5. The government's view is incorrect. The government's argument implies that sufficient legal protection is guaranteed and the right to effective remedy is preserved by having the surveillance order reviewed by the court and by giving the accused the opportunity to defend himself against the surveillance order in court proceedings afterwards.

6. This is not true for several reasons:

7. The question of whether the PTSS and the domestic courts had to rule on the merits of the applicants' request that the providers be ordered not to forward the traffic and billing data concerning the complainants to the PTSS or to other authorities or courts must be separated from the question of whether part of the fundamental rights interference associated with data retention is not to be reviewed in these proceedings because it concerns aspects of data retention related to criminal procedure.

8. The government's assumption that sufficient legal protection is ensured and the right to an effective remedy is maintained in that the surveillance order is reviewed by the court and the defendant is subsequently given the opportunity to challenge the surveillance order in a court proceeding is incorrect. If, in specific criminal proceedings, a surveillance order is issued requiring the provider to transmit metadata stored to the law enforcement authorities, the individuals whose data this affects are initially not informed of this. Legal protection is granted in principle within the framework of the Swiss Criminal Code (SCC). However, this legal protection is only provided retrospectively – if at all – after the law enforcement authorities have already become aware of the data and they have been able to use the data as evidence. Moreover, this legal protection is not afforded to all persons to whom the metadata relate.

9. In any case, the accused has the possibility to obtain legal protection against the surveillance order after the fact. However, the criminal proceedings are already well advanced at this point, and the data obtained from the surveillance has already been used as evidence in the criminal investigation and, as a rule, has already been held against the accused. The surveillance

data has been mixed with other evidence, and the accused person will be primarily concerned with defending himself against the criminal charges brought against him. The possibility of subsequently claiming that the surveillance measures were unlawful will take a secondary role.

10. In its considerations, however, the government also disregards the fact that the transmitted data regularly concern other persons than just the accused, including law-abiding third persons. It is not ensured in the Swiss Criminal Procedure Code (CrimPC), nor is it guaranteed in practice, that these third parties subsequently become aware of the surveillance order and have the opportunity to challenge it in court. Under certain circumstances, the identity of these third parties may not even be known to the prosecuting authorities. For all these persons, the criminal procedure does not guarantee any possibility of appeal against the surveillance order and the use of the metadata concerning them in criminal proceedings. The possibility of appeal mentioned by the government (para. 99.) therefore exists only theoretically in many cases.

11. Insofar as there is a possibility to lodge an appeal after the fact, the disadvantages resulting from the fact that the appeal can only be lodged after the fact, when the authority, namely the public prosecutor's office, has already received the data and has been able to use it, must not be ignored. The fact that the authority has obtained the data and the associated interference with fundamental rights cannot be undone by this possibility of lodging a complaint.

12. This is particularly serious when journalistic source protection is affected. Journalistic source protection not only protects the content of the communication between the journalist and the source, but also the fact that a journalist communicates with his or her source. The metadata transmitted by the provider in the context of a surveillance order may indicate or prove that a journalist communicates with his or her source. In this context, the source may also be the accused person. If the persons who are subject to the protection of sources are only subsequently granted the possibility to take action against the surveillance order, they cannot thereby a priori achieve that the knowledge already obtained by the public prosecutor's office that, when and via which channels the journalistic source communicated with the journalist can be eliminated again.

13. In addition, the journalist in particular, if he is not himself an accused but is involved in the data transfer as a third party, is in most cases not even given the opportunity to take action against the surveillance order. The same applies to an involved source who is not himself a defendant. In these cases,

the legal protection after the order of a surveillance measure does not come into effect at all.

14. It should also be noted that the court involved in approving the surveillance order is not necessarily aware that the surveillance concerns data that is subject to journalistic source protection. In this respect, too, the court will not be in a position to take measures to ensure journalistic source protection.

15. The protection of sources cannot be safeguarded if data retention is allowed. Article 271 SCC does not provide journalists with effective protection of their fundamental rights. On the one hand, the decisive information, namely that, where and via which channel a journalist has communicated with another person, lies in the retained data itself. Insofar as the communication partner is a protected source, the corresponding information is directly available to the law enforcement authorities when the information on the data retention data is obtained. The law enforcement authorities thus obtain knowledge of the contact between a journalist and another person without further ado. If this other person is a source of the journalist, the protection of sources is thus eliminates. On the other hand, the journalist is less thoroughly protected than, for example, the lawyer. In the case of lawyers, all communications within their professional sphere are protected by the attorney-client privilege. In the case of journalists, on the other hand, the protection only applies to their source, not to any other contacts, since they only have a right to refuse to testify to this extent. Paradoxically, the enforcement of the regulation according to Art. 271 para. 3 SCC in the case of the journalist would require that the authority that carries out the elimination of the data has knowledge of the fact that the data concerns a journalistic source, i.e. precisely of the fact that is supposed to remain hidden from it. A subsequent removal of the corresponding data does not change this,. The corresponding data may no longer be in the files afterwards. The knowledge of who the journalist's source is has already reached the minds of the law enforcement agencies involved. The protection of journalists' sources, in which a central issue is who communicates with whom, shows how drastic it can be when data retention data reaches the law enforcement authorities. In the case of journalistic source protection, it is primarily crucial that no corresponding metadata are disclosed that would allow conclusions to be drawn about the communication partners. This can only be guaranteed if such metadata are not stored at all.

16. In addition, selective deletion of data subject to the journalist's right to refuse to testify is sometimes not possible at all. In practice, partial removal of data is not possible or only possible to a limited extent. In principle, data integrity must be maintained. Another problem is that the person under surveillance may have an interest in ensuring that communication data with

persons subject to secrecy are also included in the investigation. If such data are immediately segregated and destroyed, they can no longer be introduced into the proceedings, even if the person concerned later requests this. Finally, it happens again and again that communication partly concerns protected secrets, but also contains passages that are open to further analysis. However, the partial deletion of individual communication processes is not technically possible and would also be questionable due to the associated risk of misuse. In any case, an order by the public prosecutor's office is required, which in turn presupposes that the public prosecutor's office has previously taken note of the relevant data (THOMAS HANSJAKOB, StPO-Kommentar, Art. 271 StPO N 15 ff.). Thus, the protection of professional secrets, in particular the attorney-client privilege, is also not guaranteed.

17. Because surveillance measures are secret, the journalist concerned is initially unaware of them, but may be informed about them afterwards, which in practice is not guaranteed in every constellation, especially if the journalist is not under surveillance himself, but only a third party. If data from an order is used in which the journalist himself is not the subject of the measure, but data concerning him is released, he is not informed. The journalist does not even have a right of appeal, which contradicts Article 13 of the Convention. If the court carries out the segregation before the persons concerned are informed about the measure, the journalist is not involved in the procedure, regardless of whether it affects him as a monitored person or otherwise. In this situation, the guarantee of source protection is the responsibility of the other parties involved, i.e. the state attorney and the court. Due to the relative nature of the journalist's right to refuse to testify, the ordering authority may become aware of facts whose protection is intended under Art. 264 para. 1 SCC. It is also not necessarily obvious to the authorities involved that the protection of journalistic sources is affected. Finally, there is an actually insoluble problem in that, on the one hand, the authorities involved would have to realize that the protection of sources could be affected in order to safeguard it. For this, however, they would have to have certain knowledge of the data, which in the case of source protection can lead precisely to its violation (BaslerKomm, JEAN-RICHARD-DIT-BRESSEL, Art. 271 StPO N 10 f.; THOMAS HANSJAKOB, StPO-Kommentar, Art. 271 N 8, N 14 f.; SCHMID, StPO Praxiskommentar, Art. 271 N 9; BASLERKOMM/BOMMER/GOLDSCHMID, Art. 264 StPO, N 58 f.; VIKTOR GYÖRFFY, Quellenschutz im Strafprozess, in: medialex 6/16 as well as medialex Jahrbuch 2016, pp. 79 ff, para. 24 ff.).

18. An instructive example of the fact that journalistic source protection with regard to the use of surveillance data in criminal proceedings, including the use of metadata from data retention, is not guaranteed in practice in

Switzerland is the following case: In criminal proceedings conducted against various parties, an accused person, the former Federal Councillor Christoph Blocher, appealed all the way to the Federal Supreme Court, citing the right to journalistic protection of sources, against the use of data on communications between him and journalists in the criminal proceedings. The Federal Supreme Court upheld his complaint and held that the data is protected by journalistic source protection even if it is seized from the accused person (BGE 140 IV 108). At a later point in time, Christoph Blocher and the journalist Urs Paul Engeler, who had communicated with Christoph Blocher during the period under investigation, discovered that data relating to this remained stored by the law enforcement authorities. Some of this data became public. Among other things, the Tagesanzeiger published an article on March 29, 2016, entitled «Hildebrand-Affäre: Blocher und Köppel in Dauerkontakt» («Hildebrand affair: Blocher and Köppel in permanent contact») which reported extensively on the contact between Christoph Blocher and Urs Paul Engeler, who was working at «Weltwoche» at the time, as well as other journalists at Weltwoche. The contacts between Christoph Blocher and the journalists were also partly elicited from communication data (medata and content data) between Christoph Blocher and other persons accused in the criminal proceedings, which contained references to the communication between Blocher and the journalists. It turned out that some of the data on communications between Christoph Blocher and the journalists had not been removed from the files of the criminal proceedings against Christoph Blocher. This was due, among other things, to the fact that the Federal Court had not ruled in this appeal on the question of whether the meta data from the retroactive telephone surveillance could also be used. In addition, other separately kept files against other accused persons also contained references to communications between Christoph Blocher. In its ruling, the Federal Supreme Court had not dealt with these data in other files. The data, which was subject to journalistic source protection, from the other files had never been removed. The state attorney had explained this to the media by saying that the other defendants had not asked for these files to be removed, but had accepted that the state attorney would evaluate the data its entirety. Urs Paul Engeler was never informed throughout the criminal investigation that these files contained data relating to his journalistic activities, and he was never given the opportunity to object to these data being used in the criminal investigation (DOMINIQUE STREBEL, Prekärer Quellenschutz im digitalen Zeitalter, April 11, 2016 [https://dominiquestrebel.wordpress.com/2016/04/11/prekaerer-quellenschutz-im-digitalen-zeitalter/]; interview on persoenlich.com with Urs Paul Engeler [https://www.persoenlich.com/medien/nicht-der-leiseste-aufschrei-in-der-medienbranche]; GYÖRFFY, loc. cit, para. 2 f.; Tages-Anzeiger, March 29, 2016, «Hildebrand-Affäre: Blocher und Köppel in

Dauerkontakt» [https://www.tagesanzeiger.ch/hildebrand-affaere-blocher-und-koeppel-in-dauerkontakt-281294163036]).

19. Thus, the preservation of the right to journalistic source protection cannot be guaranteed by the possibility mentioned by the government that the surveillance order will be subject to judicial review and that a subsequent challenge to the order will be possible. The journalist must reckon with the fact that data retention data, which accrues through communication with sources, will be used in criminal proceedings and thus reveal his sources. The protection of sources is thus compromised by data retention and can no longer be guaranteed as soon as the journalist uses means of communication that are subject to data retention. The impairments of fundamental rights associated with data retention thus weigh particularly heavily for a journalist, including the chilling effects contained therein. Data retention thus has a lasting impact on his work and his way of working, especially since as a journalist he is essentially dependent on communication and the use of modern communication channels. The journalist is faced with the choice of giving up source protection in communications subject to data retention, or to stop using these forms of communication. The right to source protection and freedom of the media is thus violated. In the debate on the reintroduction of data retention in Germany, weighty dissenting votes have therefore been cast, pointing to the incompatibility with journalistic source protection (GYÖRFFY, loc. cit., para. 39 m.w.h.; https://netzpolitik.org/wp-upload/2015-05- 15_BMJV-Referentenententententwurf-Vorratsdatenspeicherung.pdf; http://www.djv.de/fileadmin/user_upload/Infos_PDFs/Gemeinsame_PM_11_06_15.pdf).

20. Insofar as the government states that the providers have the option of administrative proceedings against orders of the PTSS (para. 4.), it must be countered that this is not able to close the gaps and inadequacies of the legal protection of the persons concerned. The administrative procedure mentioned by the government does not have the purpose of ensuring that the providers, instead of a person affected by the surveillance, safeguard his or her interests protected by fundamental rights. It is questionable to what extent the providers could even recognize that the fundamental rights of persons affected by the surveillance are affected, and it is not guaranteed and does not occur in practice that providers defend themselves against surveillance orders on such grounds. Providers also face a conflict between the obligations imposed on them by the law, which the PTSS requires them to comply with, and the interests of their clients and of third parties in preserving their right to respect for private life.

21. The government further argues that metadata can only be disclosed to the authorities on the basis of an order to monitor telecommunications and that such a order does not exist. However, as stated by the applicants, it appears necessary that the disclosure of metadata concerning them to providers cannot occur at all. Neither the complainant nor the PTSS can know whether this will be the case after the filing of the complaint. Only if there is an instruction that providers may not metadata concerning them to the service or other authorities or courts is there certainty that this cannot occur. In addition, there are also forms of release of metadata to law enforcement and the intelligence service that the applicants would never even become aware of. In the case of law enforcement, this concerns, for example, the «Antennensuchlauf» ( ), where in practice most of the persons whose antenna data are disclosed to law enforcement are never informed about it. The applicants would never be informed about the disclosure of metadata to the intelligence service in certain constellations, which are defined in Art. 33 para. 2 IntelSA (necessary so as not to jeopardise an ongoing information gathering measure or ongoing legal proceedings; necessary due to another overriding public interest in order to safeguard internal or external security or Swiss foreign relations; notification could cause serious danger to third parties the person concerned cannot be contacted)

22. The applicants thus have a sufficient actual interest that merits protection that the domestic procedure ensures that the providers do not forward the traffic and billing data concerning them to the PTSS or other authorities or courts. This is the only way to ensure that this data cannot be used in criminal proceedings and that the use of this data violates their fundamental rights. In particular, journalistic source protection can only be guaranteed in this way. The actual interest that merits protection, that it is ensured that the stored metadata do not flow into criminal proceedings in violation of their fundamental rights, can only be safeguarded by addressing the complainants' request in this regard substantively. The request that the providers be instructed not to forward the traffic and billing data concerning them to the PTSS or other authorities or courts should therefore have been dealt with in the domestic proceedings. By failing to do so, the applicants' right to effective remedy under Art. 13 of the Convention has been violated with respect to the violation of Art. 8, Art. 10 and Art. 11 of the Convention.

23. In general, with regard to the complaints which have been raised by the complainants, it should be considered for what purpose the providers have to keep the metadata. The metadata are kept so that they can be used in criminal proceedings and by the intelligence service. In order to examine which fundamental rights are violated by the retention of the metadata and how grave these violations are, it is thus imperative to also take into account under which conditions and for which purposes the retained data can

subsequently be used by the authorities and which legal provisions apply in this context. The government's statements as to which complaints were rightly not examined in the national proceedings thus prove to be incorrect. All objections should have been examined in the national proceedings.

24. In the national proceedings, the applicants' request that the providers be instructed not to forward the traffic and billing data concerning them to the service or to other authorities or courts has not been dealt with in substance. The Government takes the view that this is correct. However, the Federal Supreme Court's finding, cited by the Government in this regard, that the appellants had inadequately substantiated their appeal to the Federal Supreme Court on this point and had not addressed the Federal Administrative Court's considerations on this issue is incorrect.

25. In the appeal to the Federal Supreme Court, the applicants pointed out in particular that the Federal Administrative Court acknowledged that the wording of Art. 13 para. 1 let. a BÜPF, which regulates and restricts the review power of the PTSS with regard to aspects of criminal procedure, does not a priori exclude a (comprehensive) review power in terms of administrative law (No. I. 13., p. 5 f. of the appeal of 15 December 2016).

26. In order to substantiate that the request would have had to be dealt with substantively in its entirety by the PTSS and the Federal Administrative Court, i.e. including request 2, the applicants submitted the following to the Federal Supreme Court: Since the storage of the data was contrary to fundamental rights, the use of the stored data was equally contrary to fundamental rights. Thus, in the form of a corresponding instruction to the provider, it had to be ensured that stored data were not used. The PTSS had issued an order with regard to request 1. The Federal Administrative Court had dealt substantively with the appeal against this order and had ruled on it in the contested judgment. Request 2 would also have had to be decided by the PTSS and by the Federal Administrative Court. Insofar as the Federal Administrative Court was of the opinion that it had not been able to decide substantively on this matter due to the previous decision not to appeal, it could also have annulled the respondent's decision in this respect and ordered that it be referred back to the respondent for substantive consideration. By doing neither, it had obstructed the required protection of the applicants fundamental rights and thus violated their fundamental rights (para. I. 14., p. 6).

27. In the appeal to the Federal Supreme Court, the applicants also pointed out that the Federal Administrative Court had emphasized that the law enforcement agency already receives the meta data at a time when approval of the retroactive monitoring order by the court had not yet been granted as

a rule and when no legal remedy against the monitoring order was yet available to the person concerned.

28. The complainants further argued that the Federal Administrative Court had limited its review of compliance with fundamental rights on the basis of the task of the PTSS and had subsequently largely ignored the criminal procedure aspects of data retention (E 8.5). However, it fails to recognize that the examination of the compatibility of data retention with the Convention thus cannot meet the cited requirements of the Court. The encroachment on fundamental rights lies – as the Federal Administrative Court rightly recognizes – first of all in the monitoring per se associated with the storage of the retained data without any reason. The encroachment goes beyond this, however, in that it permits the subsequent use of the retained data in any criminal proceedings. This is also the virtual encroachment on the guarantees of the Convention associated with the retention of data. In assessing the conformity of data retention, the possible later use, the manner of processing and the results that can be obtained must be taken into account, because these aspects are part of the encroachment on fundamental rights associated with data retention. The rules governing the use of data retention in the CrimPC and the competences provided for therein, namely those of the state attorney and the courts, would not change this (No. II. A. 5., p. 9).

.29 The complainants have also explained that the Federal Administrative Court was of the opinion that the relevant claims should be raised in a possible criminal proceeding, and they have explained in detail that the protection of sources and the right to protection of journalistic sources are already violated by the storage of the retained data itself and that safeguarding these fundamental rights is not guaranteed in criminal proceedings. The Federal Administrative Court's statements are thus obviously inadequate, violate the complainants, who work as journalists, in their right to be heard and in their right to an effective remedy (No. II. I., p. 52 ff.).

30. The complainants have thus sufficiently substantiated why their request that the providers be ordered not to hand over any traffic and billing data of the complainants stored in accordance with the law to the PTSS or to other authorities or to the courts should be dealt with substantially and why the request should be upheld, and in their appeal to the Federal Supreme Court they have also sufficiently addressed the reasoning of the Federal Administrative Court.

31. The complainants have also explained to all national instances why, in order to assess the violation of fundamental rights associated with the retention of data by the providers, it is also necessary to examine how these data can be

used by the authorities and what encroachments on fundamental rights are associated with this.

32. This holistic review of the fundamental rights interference associated with data retention, including the use of the data by the authorities, is also in line with the practice of the Court. In the Ekimdzhiev case (Ekimdzhiev and Others v. Bulgaria, No. 70078/12, January 11, 2022, esp. §§ 372. et seq. , §§ 376. et seq., §§ 394. et seq.), the Court reviewed the contested surveillance measures as a whole, including the storage of the data by the providers and their use by the authorities. In doing so, the Court affirmed that the mere storage of the data constitutes an interference with fundamental rights (372. et seq.) and that the access to the data by the authorities constitutes a further interference (376. et seq.). Subsequently, the Court examines the compatibility of the surveillance measures with regard to both aspects (retention by providers and access to the data by the authorities).

II. Violation of Art. 8 of the Convention

A. Interference with fundamental right

33. The Government considers that Article 8 of the Convention has not been violated. The Government rightly recognizes that the storage of metadata constitutes an interference with the applicants' rights protected by Article 8 of the Convention.

34. However, it fails to recognize the scope and gravity of this interference. Contrary to the government's view, the retention of this data constitutes a serious interference with these rights.

35. On the one hand, it must be taken into account that from such metadata far-reaching conclusions can be drawn about the applicants, in particular about whom they communicate with and how often, where they stay and where they go and – especially in combination with data available about them from other sources, but also with other general data – about their behavior and their personal and political views.

36. From a technical point of view, it should be noted that 5G technology in mobile communications allows even more precise localization than previous technologies. The Federal Council has already indicated that it intends to exploit these new technical possibilities and adapt the Ordinance on the Surveillance of Post and Telecommunications (SPTO) accordingly (https://www.digitale-gesellschaft.ch/2022/05/23/bundesrat-will-die-ueberwachung-mit-der-einfuehrung-der-5g-technologie-stark-ausbauen-stellungnahme/).

37. It must be emphasized that the retention of metadata already leads to an invasion of privacy regardless of whether or not these data are later consulted or used by authorities.

38. On the other hand, the severity of the interference associated with the retention of the data must be assessed in view of the purpose for which the providers are required to retain the data. The data is not simply retained, but specifically in order to be able to use it in a criminal investigation or for the other purposes stipulated by the law. This must be taken into account when assessing the gravity of the encroachment on fundamental rights. It should be remembered that very detailed regulations exist as to what data must be retained and the form in which it must be supplied to the PTSS or the law enforcement authorities. (see Ekimdzhiev and Others v. Bulgaria, § 375.)

39. The European Court of Justice (ECJ) has ruled in detail on the content and seriousness of the interference with private and family life resulting from data retention in several decisions. It states that traffic and location data may contain information about a variety of aspects of the private life of the data subject, including sensitive information such as sexual orientation, political opinions, religious, philosophical, social or other beliefs, and state of health. From the totality of these data, it is possible to draw very precise conclusions about the private life of the persons whose data have been stored, such as habits of daily life, permanent or temporary places of residence, daily or other rhythmical changes of place, activities carried out, social relations of these persons and the social environment in which they socialize. These data allow, in particular, the establishment of a profile of the data subjects, which constitutes information that is as sensitive in terms of the right to respect for private life as the content of the communications themselves (judgment of the ECJ of 20 September 2022, C-793/19 and C-794/19, *SpaceNet AG and Telekom Deutschland GmbH*, para. 61). Consequently, the storage of traffic or location data that can provide information about the communications of the user of an electronic communications medium or about the location of the terminal equipment he or she uses is serious in any case, regardless of the length of the storage period and the amount or type of data stored, provided that the data set is capable of allowing very precise conclusions to be drawn about the private life of the data subject or data subjects (ECJ judgment of September 20, 2022, C-793/19 and C-794/19, *SpaceNet AG and Telekom Deutschland GmbH*, para. 88).

40. The storage of the metadata by the providers and the (potential) use of this data by the law enforcement authorities and the intelligence service, as permitted by the Federal Act on the Surveillance of Post and Telecommunication (SPTA), the CrimPC and the IntelSA as well as in the

associated ordinances, thus constitute a serious encroachment on the applicants' right to private life. As explained, the seriousness of this encroachment on fundamental rights and its permissibility must be comprehensively examined in these proceedings, also with regard to the encroachment on fundamental rights resulting from the use of the data by the authorities.

B. Provided by law

41. The legal provisions on which the storage of metadata and their use in criminal proceedings are based are not sufficiently specific. The subjects of the law cannot adequately assess which data exactly are collected and under which circumstances they can be used and how.

42. Moreover, the practice of storing the metadata and their use by the authorities is partly not based on the law (in the sense of a law passed by the Parliament), but substantially also on regulations and guidelines. Regulations and guidelines are not a sufficient legal basis. They are not sufficiently democratically legitimized and, in some cases, not sufficiently accessible and comprehensible to those subject to the law. This applies in particular to the monitoring of foreign address resources («Kopfschaltung», in which telecommunications traffic from the entire Swiss network is monitored for a specific foreign number [THOMAS HANSJAKOB, Überwachungsrecht der Schweiz, Zurich 2017, n. 392]) and «Antennensuchlauf» (dragnet searches in antenna data). Since the collected data could one day be used by the authorities on the basis of these regulations and guidelines, it is relevant in the context of this procedure to examine whether the use of metadata to be justified on the basis of ordinances and guidelines.

43. The so-called «Antennensuchlauf» represents a dragnet search in stored antenna locations (see 1B_376/2011 as well as SIMON SCHLAURI, Fernmeldeüberwachung à discrétion?, in: sic! 2012, p. 238, p. 240 f.). A person may at most be aware that every time he uses his cell phone (or the cell phone is activated for certain functions that the user may not even be aware of), the location of the antenna, including the main beam direction, is stored and that his effective location is thus recorded very precisely, possibly to within a few meters. However, they will hardly be aware that this data can be used to include them in a dragnet search if the law enforcement agency wants to know who has been at a certain location at a certain time during the last six months as part of a corresponding criminal investigation. Moreover, the dragnet search of stored antenna locations can only be based on a provision of an ordinance. There is no law in the formal sense that would regulate this measure in detail. It therefore does not have a sufficient legal basis, especially since it represents a serious encroachment on

fundamental rights. In addition, most of the persons whose data are included in such a dragnet are not subsequently informed about the use of their data.

44. Data retention is a complex, highly technical matter. Some of the details are not regulated in the law itself, but in subordinate ordinances. In these ordinances in particular, the regulations are formulated in a very technical manner and are primarily addressed to the providers. For those subject to the law, this makes it difficult to determine what data is specifically affected and what can be read from the data collected. For a legal basis to be sufficient, it must also be clear to those subject to the law, so that they are aware of the conditions under which they may be affected by the law and what this could mean for them in concrete terms. The regulation of data retention in the SPTA, the CrimPC and the IntelSA does not meet these requirements. The conditions for the use of the data by the law enforcement authorities are, moreover, as stated elsewhere are too broad and too vague and thus do not limit the use in a clear and effective manner.

C. Legitimate purpose

45. It is correct that the retention of metadata is done for the purpose of using them for possible future criminal proceedings, for the execution of mutual legal assistance requests, for the search and rescue of missing persons as well as for information gathering by intelligence services.

46. With regard to the use in criminal proceedings, however, it must be pointed out at this point that according to the law and practice, the use is not limited to the prosecution of serious or even the most serious crime, but such metadata are also used for the prosecution of crimes of lesser gravity.

47. The access of the intelligence service to retained data is, as stated elsewhere, is not sufficiently precise and effective.

48. The purpose invoked by the government is thus defined too broadly and too imprecisely in its concrete form in the law, which clearly relativizes its significance.

49. The government also mentions the purpose of protecting the rights of third parties. It mentions, among other things, the state's obligation to ensure that Internet providers disclose the identity of persons involved in the dissemination of offensive and abusive material (para. 60.). In any case, however, this does not justify the obligation of providers to retain the accruing metadata of their customers indiscriminately. Rather, it is only a question here of the data available at the provider regarding the identity of persons who use their Internet access as customers.

D. Necessity

50. The use of metadata to pursue the stated purposes, as provided for by the law and carried out in practice, does not appear to be necessary to achieve the aforementioned purposes.

51. With respect to necessity, a distinction must be made between whether law enforcement authorities should in principle be allowed to use surveillance data and whether it seems justified that virtually all metadata of all persons in a country must be kept for months as a preventive measure in order to possibly use them later in criminal proceedings or for intelligence purposes.

52. The interception of postal and telecommunications traffic per se for law enforcement and public security purposes may be justified, provided that it is subject to certain conditions and that there are adequate safeguards against excessive or improper use.

53. However, this is to be distinguished from the retention of metadata of all persons without any reason.

54. The ECJ has dealt with this question of principle in detail and correctly concluded that a general and indiscriminate retention of traffic and location data as a preventive measure to combat serious crime and to prevent serious threats to public security violates the right to respect for private and family life. A general and indiscriminate retention of metadata does exceed the limit of what is necessary, is disproportionate and cannot be considered as justified in a democratic society. The ECJ has confirmed this in several decisions and has also repeatedly addressed the conditions under which and the situations in which metadata can be stored and used by the authorities. A regulation would be permissible that allows the targeted retention of traffic and location data as a preventive measure to combat serious crimes, provided that the retention of data is limited to what is absolutely necessary in terms of the categories of data to be stored, the electronic means of communication covered, the persons affected and the intended duration of the retention. The national regulation in question must, firstly, provide for clear and precise rules on the scope and application of such a data retention measure and establish minimum requirements so that the persons whose data have been retained have sufficient guarantees to ensure effective protection of their personal data against the risk of misuse. In particular, it must specify the circumstances and conditions under which a data retention measure may be taken as a preventive measure, thereby ensuring that such a measure is limited to what is absolutely necessary. Second, while the substantive conditions that a national regulation allowing the retention of

traffic and location data as a preventive measure in the context of the fight against crime must meet in order to ensure that it is limited to what is absolutely necessary may differ depending on the measures taken to prevent, investigate, detect and prosecute serious crimes, the retention of data must always satisfy objective criteria that establish a link between the data to be retained and the objective pursued. In particular, these conditions must be suitable in practice to effectively limit the scope of the measure and, consequently, the categories of persons concerned. In limiting such a measure with regard to the categories of persons and situations potentially concerned, the national regulation must be based on objective connecting factors which make it possible to cover categories of persons whose data are likely to reveal at least an indirect connection with serious crime, to contribute in some way to the fight against serious crime or to prevent a serious threat to public security. Such limitation can be ensured by a geographical criterion if the competent national authorities assume, on the basis of objective evidence, that there is an increased risk of such acts being prepared or committed in one or more geographical areas. In its decision of April 8, 2014 , the ECJ declared Directive 2006/24/EC on data retention invalid because it was not limited to what was absolutely necessary and was therefore disproportionate. Among other things, it reasoned that the directive generally covers all persons, all electronic communications and all traffic data, without providing for any differentiation, limitation or exception. In particular, it covers all persons who use electronic means of communication, without these even indirectly or remotely giving rise to criminal prosecution. Nor does the directive require a connection between the retained data and the threat to public security. Thus, it is not limited to data of a particular period, area, or group of persons who may be involved in serious crime in any way or who may otherwise contribute to the prevention or prosecution of such crime. In addition, the Directive provides for a minimum period of six months for data retention, without any distinction being made between categories of data according to their possible usefulness for the objective pursued or on the basis of the data subjects (ECJ judgment of April 8, 2014 C-293/12 and C-594/12, *Digital Rights Ireland*, para. 57 et seq.). The ECJ confirmed this case law in further rulings on data retention, concluding that a national regulation providing for the general and indiscriminate retention of data does not stand up to European Union law and, in particular, the Charter of Fundamental Rights for the reasons already mentioned (esp. ECJ judgment of 6. October 2020, C-623/17, C-511/18, C-512/18, 520/18, *Privacy International, La Quadrature du Net and Others, French Data Network and Others*; judgment of the ECJ of 21. December, C-203/15 and C-698/15, *Tele2 Sverige AB , Post- och telestyrelsen ;* ECJ judgment of September 20, 2022, C-793/19 and C-794/19, *SpaceNet AG and Telekom Deutschland GmbH* ; judgment of September 20, 2022, C-339/20 and C-397/20, *VD and SR*). However, according to the ECJ, the

latter does not prohibit the member states from enacting a regulation that allows targeted retention of traffic and location data, provided that this is limited to what is absolutely necessary in terms of the categories of data, the electronic means of communication, the group of persons and the retention period. In order to meet these requirements, the national regulation must be clear and precise and contain sufficient guarantees to protect against the risk of misuse. It must specify the circumstances and conditions under which a data retention measure may be ordered. In particular, it must be based on objective indications that make it possible to record those persons who have at least an indirect connection to serious crimes. Such a limitation can also be ensured by a geographical criterion if there are objective indications that there is an increased risk of the preparation or commission of criminal acts in certain areas (judgment of the ECJ of December 21, 2016 C-203/15 and C-698/15 *Tele2 Sverige, Post- och telestyrelsen*, para. 108 et seq.). In another ruling (ECJ judgment of September 20, 2022 C-793/19 and C-794/19, SpaceNet AG and Telekom Deutschland GmbH), the ECJ stated that it appears justified,

- to permit, for the protection of national security, an order requiring providers of electronic communications services to retain traffic and location data in a general and indiscriminate manner when the Member State concerned is faced with a serious threat to national security which is considered to be real and present or foreseeable. Such an order may be controlled by a court or an independent administrative body and may be issued only for a period limited to what is absolutely necessary, but renewable if the threat persists;
- to provide for the targeted retention of traffic and location data for a period limited to what is absolutely necessary, but extendible, for the purpose of protecting national security, combating serious crime, and preventing serious threats to public security on the basis of objective and non-discriminatory criteria based on categories of data subjects or by means of a geographical criterion;
- provide for general and indiscriminate retention of IP addresses assigned to the source of a connection, for the same purposes, for a period limited to what is absolutely necessary; provide for general and indiscriminate retention of data relating to the identity of users of electronic communications, for the purpose of protecting national security, combating crime and protecting public safety;
- for the purpose of combating serious crime and, a fortiori, for the protection of national security, to require providers of electronic communications services to immediately secure, for a specified period of time, the traffic and location data available to them.

55. The ECJ further held that such national legislation must also ensure, through clear and precise rules, that the storage of the data in question complies with

the substantive and procedural conditions applicable to it and that the data subjects have effective safeguards to protect them against the risk of misuse (ECJ judgment of September 20, 2022, C-793/19 and C-794/19, SpaceNet AG and Telekom Deutschland GmbH) .

56. The ECJ has thus shown that a restriction requiring the respect of the right to respect for private and family life does not exclude the use of data from surveillance measures, including metadata, for the purpose of law enforcement and safeguarding national and public security, as long as it appears necessary and proportionate.

57. Likewise, the case law of the ECJ shows unequivocally that it appears to be necessary to start with the storage of metadata data at the providers by not permitting an unprovoked, general and indiscriminate retention and that, apart from narrowly defined exceptions, it appears to be impermissible to store them in advance for the above-mentioned purposes.

58. The government refers several times to the guarantees that must be ensured in connection with surveillance measures. It is true that a surveillance program can only be permissible if corresponding safeguards exist. But not every conceivable surveillance program that strives to provide such safeguards is permissible. Regardless of the safeguards, for a monitoring program to be lawful, it must be deemed necessary and proportionate.

59. In order to justify the storage of a large amount of data of law-abiding persons without any reason, it is not sufficient that the state claims that these data could serve it in the investigation of crime and for the protection of national or public security or for the protection of the rights and freedoms of others. The claim that the data could be useful for these purposes can easily be made. If any conceivable surveillance useful for these purposes were deemed permissible, then this could be used as justification for total surveillance of the entire population. It could always be claimed that this is the only way to gather specific data that are relevant to the protection of the interests enumerated in Art. 8 of the Convention.

60. The mere circumstance that the actual use of the collected data by the state for these purposes is subject to further limitations is not able to limit their prior storage throughout. It is not justified to subject the entire population to permanent surveillance, up to and including total surveillance, in order to have this data available later in individual cases in which a crime may have been committed, national or public security may be threatened, or other persons may be threatened in their rights and freedoms.

61. The argument put forward by the government is thus not viable. It does not provide an effective limitation on the collection of surveillance data as such, but could be used to justify ever more extensive surveillance of the entire population, up to and including total surveillance. It is therefore necessary, but not necessarily sufficient, that the use of accumulated data be subject to a system of safeguards. Rather, in order to maintain the requirement of necessity and proportionality, there must also be sufficient limits on what data may be stored at all. Otherwise, total surveillance of the population can, in principle, be justified. However, excessive data collection cannot be justified under any circumstances, not even by any kind of safeguards related to the use of these data.

62. A law-abiding person must in principle be able to claim that his right to respect for his private and family life, his home and his correspondence is guaranteed and must be in a position to exercise this right free from surveillance measures. The storage of metadata of their communication without any reason seems disproportionate and therefore not justified.

63. As explained above, the ECJ has shown in a number of decisions that the general and indiscriminate retention of metadata for the purpose of fighting serious crime and preventing serious threats to public security is not necessary and proportionate and violates the right to respect for private and family life. The ECJ has also shown that and under which conditions the use of metadata, within narrow limits also those that are retained, is permissible.

64. It should be noted that there are various procedures that limit the use of metadata to those that have accrued in close temporal and factual connection with the crime under investigation and which sufficiently serve the public interests. For example, there is the procedure known in Germany as «quick freeze». In this process, existing metadata is immediately saved as soon as there is an urgent suspicion of a crime. A short time later, a decision can be made as to the extent to which an initial suspicion gives cause to use the secured data in specific criminal proceedings. The big difference here is that it is only the urgent suspicion of a crime that gives rise to the encroachment on fundamental rights in the first place. In order to ensure the effectiveness of this procedure and to give those affected by it, including the providers, sufficient legal certainty, it is possible to precisely regulate the prerequisites and details of the procedure for the «quick freeze» , including the way in which existing metadata are to be made available by the providers. Another component of this procedure is that the provider is instructed to freeze existing data as soon as a suspicion of a crime arises, and the decision on the permissibility of using the data is made at a later point in time. In this respect, this procedure prevents data loss.

65. Since the metadata are initially generated by the providers for technical reasons and many of these metadata are also stored by the providers for a certain period of time for technical reasons, and since the procedure for the «quick freeze» can be regulated as explained, it will be possible to use data retroactively with this procedure (contrary to the government's explanations, para. 70).

66. By contrast, with data retention according to the laws in Switzerland, all persons participating in postal and telecommunications communications suffer an encroachment on fundamental rights. As far as the persons affected are concerned, the encroachment thus becomes universal. This does not appear to be necessary. With «quick freeze», data retention also does not go back as far as six months, which represents a minor encroachment on fundamental rights and appears to be sufficient, especially since it is evident from the statistics kept by the PTSS that in most cases the law enforcement authorities only need data that has accrued in a short period of time (cf. SwiNOG Federation media release of June 16, 2013, https://www.digitale-gesellschaft.ch/2013/06/13/neue-statistiken-vorratsdatenspeicherung-ist-auch-hinsichtlich-der-vorhaltedauer-unverhaltnismassig/). In any case, it is clear that data retention is associated with nationwide impact for all persons, although the data of the vast majority of persons is never used.

67. The indiscriminate and indiscriminate retention of metadata, as permitted by law in Switzerland, can thus not be considered necessary and proportionate and violates Art. 8 of the Convention.

68. There are also no sufficient guarantees that would provide effective protection against the metadata stored being used excessively and that the fundamental rights of the persons concerned are not violated. In particular, the legal protection provided for by law is clearly inadequate and, contrary to the government's claims, cannot provide the necessary protection.

69. The law permits the use of stored metadata for the prosecution of felonies, misdemeanors, further for the prosecution of violations under Article 179septies SCC (misuse of a telecommunications installation) as well as generally for the investigation of any crimes committed via the Internet (Art. 14 para. 4 SPTA). Thus, the law also permits the use of metadata for the prosecution of crimes of minor gravity. The law has a precedent-setting effect on practice in that it also declares the use of metadata for less serious crime to be permissible. By not limiting the use of the metadata to the most serious crime, the legal regulation and the practice are not proportionate and thus violate fundamental rights.

70. Judicial review and the possibilities created in the law for data subjects to subsequently appeal the order for surveillance are not sufficient. First, the law allows for excessive use of the data. Second, in practice, not all persons whose data from surveillance is used are given the opportunity to subsequently object to it. Only the accused is always informed of the order after the fact.

72. The inadequate legal protection affects journalists and their sources in particular, who enjoy journalistic source protection. This protection of sources is violated by the statutory possibility of storing metadata and using it in criminal proceedings and by the lack of effective legal protection against unjustified interference with the right to journalistic protection of sources.

73. It should be noted that the question of necessity has not been sufficiently reviewed in the domestic proceedings. In this context, the government quotes from the judgment of the Federal Supreme Court (para. 74.). It must be pointed out to the contrary that the Federal Supreme Court effectively did not review and justify the necessity of retroactive surveillance. First and foremost, the Federal Supreme Court referred to the fact that such retroactive surveillance was intended by the legislator and should therefore be accepted. To what extent the retention of such data is effectively necessary, the Federal Supreme Court did not substantiate therewith. In particular, the Federal Supreme Court did not explain why this should be necessary and proportionate for the prosecution of even non-serious crime.

E. Type of data recorded and stored

74. The government states that the applicants claim that they feel influenced in their behavior by the fact that their metadata is stored by the providers and that this data could be used for surveillance purposes (para. 67.).

75. The applicants' claim to be influenced by the possibility that the stored metadata could be used for surveillance purposes is very well founded. Already the storage of the data per se at the provider affects their right to respect for their private and family life, their home and their correspondence. A concrete use of the metadata for surveillance purposes would take place without the applicants being able to determine this. The possibility of subsequently challenging the order for surveillance does not ensure sufficient protection of their fundamental rights, as explained elsewhere. As a result, applicants are inevitably confronted with the question of how to adapt their communications behavior to the fact that the metadata of communications are retained electronically by their providers and may later be released to law enforcement agencies or the intelligence service. These authorities may use data to accuse applicants of committing a crime, endangering security, or

interfering with the rights of others. Even if no such accusation against the complainant is associated with the use of the data (for example, if a person is recorded as a third party or because he or she uses the same connection as a target), the use of the stored data by the state is associated with a serious interference with the right to respect for private and family life.

76. The applicants have also specifically shown how and for what reasons data retention influences their behavior (for more details, please refer to para. 102 ff. below).

77. As explained, the collection of metadata as well as the use of these data by the authorities according to the legal norms in Switzerland involves a serious interference with Art. 8 of the Convention.

78. From a technical point of view, content data is also partly stored with data retention, and there are data where pure metadata and content data cannot be distinguished from each other. In the case of SMS messages, for example, data retention also stores the content of the SMS (see submission by Müller Müller Rössner to the Federal Constitutional Court of November 6, 2015 [documentation at http://www.mueller-roessner.net]).

79. When assessing the scope of the data retained with data retention, it must be taken into account that, when used by the authorities, they can be linked to other data, private data and also generally accessible data, including data of other persons. These data may originate from surveillance as well. Further data can be obtained through other investigative actions, namely with other criminal procedural coercive measures, in particular seizure or edition of data carriers or data. This can be further data to the data held in the data retention, namely content data, such as the content of an email, a voicemail message, a chat message. This data can accrue on a device used, namely a cell phone, and can be read from there. Apps on computers, cell phones and other devices are increasingly used for communication. The use of these apps generates content data and metadata that are generated on the relevant devices and remain stored, at least in part. At the same time, depending on the device and communication channel used, retained data is also generated. This is particularly the case if the data channel of a mobile communications provider is used for communication. Since such apps are used very often, especially on cell phones, their use sometimes generates enormous data traces. Other data that can be used may, for example, come from house searches, from the hard drive of a seized computer, from a mobile phone or from video surveillance. It is also possible to make disclosure requests to third parties, such as providers of Internet services, employers, government agencies, chain stores, banks, credit card companies

or online stores. Data on surfing behavior, data from social media, e-mails, and data on purchases and payments can be obtained in this way.

F. Systematic collection and storage of secondary data

80. The necessity of an encroachment on fundamental rights would have to be proven by the state. The effectiveness of data retention would have to be empirically substantiated. Citing individual cases from case law is no substitute for this, since such cases do not permit an overall assessment of effectiveness and, moreover, it will regularly remain open to what extent the data retention was effectively indispensable for solving a case or what decisive contribution it made. Data retention data will hardly ever be the only available evidence, and in individual cases the question also arises as to which other investigative approaches have been pushed into the background or not pursued at all due to the possibility of using data retention data.

81. The effectiveness of data retention has not been empirically proven, and this strongly relativizes the weight of the public interest cited. Empirical studies do not show any significant impact on the detection rate, and a deterrent effect due to a higher risk of detection is also not demonstrable. The relevant expert opinions and studies by the Max Planck Institute for Foreign and International Criminal Law are particularly informative in this regard. After data retention was introduced in Germany and later suspended due to a ruling by the Federal Constitutional Court, it would be expected that significant differences would emerge between the time when data retention was available and the time before and after. A comparison with Switzerland, which has had data retention for a long time, could also be made. The expert opinion of the Max Planck Institute for Foreign and International Criminal Law examined these correlations, but found hardly any significant changes or differences overall. In Switzerland, there are no statistics or studies on the effectiveness of data retention, although data retention has been available in this country since 2002. (Expert opinion of the Max Planck Institute for Foreign and International Criminal Law, Freiburg i. Br., 2011, Schutzlücken durch Abfall der Vorratsdatenspeicherung? [http://www.mpicc.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.htm]). The fact that the Max Planck Institute highlights uncertainties in the data situation does not detract from the findings in the expert opinion, because it would be up to the state to prove the effectiveness of the measures and the necessity of the restrictions on fundamental rights. Empirical studies cannot be replaced by anecdotally citing individual cases as proof of the benefits of data retention, especially since individual examples cannot prove a generally existing effect. In individual cases, it will regularly be difficult to determine whether the data retention was indispensable for clearing up the crime, especially since it is not

the only evidence and the actual origin of a suspected crime is sometimes not clear. It is not uncommon to find no or only nebulous references to this in the files («Police investigations have revealed...»), and it is apparently common international practice of law enforcement authorities, particularly in the drugs field, to conceal the effective origin of the suspicion of the crime, for example by staging seemingly random police checks (cf. http://www.reuters.com/article/2013/08/05/us-dea-sod-idUS¬BRE97409R20130805, where an official of the U.S. Drug Enforcement Administration [DEA] *is* quoted on this approach, referred to as *«parallel construction», as* follows: *«Parallel construction is a law enforcement technique we use every day, It's decades old, a bedrock concept.»*).

82. In addition, it should be pointed out that not only Germany, but also many other countries, especially those belonging to the EU, which implement the ECJ's prohibition against the indiscriminate storage of metadata, do not know any data retention and cannot use any resulting metadata without this having resulted in a noticeable gap in law enforcement and intelligence activities.

83. To the extent that the government cites the Ekimdzhiev judgment and argues that the system of systematic recording and storage of secondary data was not in itself called into question there (para. 73. with reference to the Ekimdzhiev judgment, §§ 394 et seq.), it should be noted that in that case the Court did not deal in detail with the question of whether and to what extent the storage of data without any reason might be permissible. Accordingly, the Court did not determine in detail in this decision that a storage of data by providers comparable to the regulation in Switzerland could be lawful. The Court upheld the appeal in that case. In its reasoning, the Court nevertheless held that there had been a violation of Article 8, in respect of retention and accessing of communication data, finding that, as the laws governing retention and accessing communications data did not meet the quality-of-law requirement of the Convention, they were incapable of limiting such retention and accessing to what was necessary. It follows, the Court further states, that those laws do not fully meet the «quality of law» requirement and are incapable of keeping the «interference» entailed by the system of retention and accessing of communications data in Bulgaria to what is «necessary in a democratic society» (see § 420.)

G. Data protection and security

84. The government is of the opinion that the provisions it cites, in particular the provisions of data protection law, provide sufficient protection against unauthorized data processing and misappropriation (para. 77, esp. para. 93). This assessment is not correct.

85. Data retention violates a number of principles of data protection law, namely the requirement of data minimization and the prohibition of collecting data in advance, the principle of purpose limitation of data and the principle of proportionality of data processing. Data retention accumulates a very large amount of data. The data is created as a by-product of communication processes and actually serves to ensure that the desired communication can technically take place. By systematically recording and storing the data so that it can be used in subsequent criminal proceedings or by the intelligence service, it fundamentally changes its purpose. In addition, the legal basis is insufficient, as explained above. For the person concerned, who only wants to communicate with the corresponding means of communication, it is not sufficiently recognizable which data is collected and for which purpose it can be used.

86. It would be necessary for the data subject to voluntarily consent to the collection of the data after being adequately informed. This is not the case with data retention. As a data subject, one is not in a position to recognize the content and scope of data retention, even if one makes an effort to obtain the relevant information. The legal basis and the technical details are incomprehensible to laypersons, as explained. Nor does the data subject have the opportunity to consent to the collection and use of the data or to prevent it by refusing consent. Finally, the data should be deleted after the statutory period of six months. However, the violation of data protection principles by a provider does not generally have any consequences under administrative or criminal law.

87. In addition, in its practice, the Federal Court allows the data to be used even after six months have elapsed (BGE 139 IV 98 [1B_481/2012]). The obligation to delete the data after 6 months therefore does not protect the data subjects from existing metadata being released by the provider and used against them even after 6 months have expired.

88. Finally, there is no guarantee that the data will not end up abroad, for example in the context of international mutual legal assistance in criminal matters, police and intelligence cooperation, but also because a provider has its data stored abroad or due to a lack of data security. Apparently, the providers concerned do indeed manage sensitive data abroad, for example Salt (formerly Orange). This provider had outsourced the operation and maintenance of its mobile network to Ericsson, which meant that the law enforcement authorities had to obtain some of the data to be supplied by Salt from Romania (http://www.srf.ch/news/schweiz/orange-verwaltet-heikle-daten-in-rumaenien). If the data is transferred abroad, compliance with the guarantees applicable in Switzerland with regard to fundamental

rights, data protection and data security is not guaranteed. This problem cannot be brushed aside with reference to abstract regulations on data protection and data security , especially since the data located abroad is also subject to the law there and this can undermine the protection against misuse to be guaranteed (illustrative of such a problem are the decisions of the ECJ, which overturned the Safe Harbor agreement with the USA and the Privacy Shield framework: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0362; https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf). When the government points out that the regulations on data protection and data security must also be complied with when the data is transferred abroad, it must be pointed out that this cannot be guaranteed in reality.

89. It is not enough for data privacy and data security to be provided for abstractly in legal standards. Rather, data privacy and data security must be ensured in reality. This is not the case with the metadata to be stored by the providers.

90. The problem of ensuring data protection and data security is greatly exacerbated by the fact that we are dealing with a huge volume of data that has to be stored by a large number of very different providers in their own systems. The risk that such data will not be kept secure, that unauthorized persons will gain access to the data, and that leaks will occur as a result, is real and not small. For this reason, strict compliance with the requirement of purpose limitation and the requirement of data economy would be of eminent importance.

91. In reality, data security is obviously not guaranteed. Actual incidents that have become known show that this is not a hypothetical problem, but a real one. Employees of Swisscom, Salt (formerly Orange) and Sunrise have apparently sold confidential data (http://www.handelszeitung.ch/unternehmen/illegaler-datenverkauf-orange-und-sunrise-bestrafen-mitarbeiter; http://www.it-markt.ch/de-CH/News/2012/05/21/Verkauf-von-vertraulichen-Daten.aspx). At Swisscom, data that was supposed to be shredded has disappeared. This has become known after corresponding data carriers were leaked to the NZZ. On them are apparently 60 million data records containing secret numbers of 979 celebrities as well as 14,500 internal mails, contracts, project descriptions and meeting minutes. Swisscom has no explanation as to how the data could have been lost. The data of two million customers including account numbers has been stolen in a hacker attack on mobile phone provider Vodafone in Germany (http://www.nzz.ch/aktuell/schweiz/entwendete-baender-bringen-die-

swisscom-in-noete-1.18151998;
http://www.nzz.ch/aktuell/schweiz/brisante-prominenten-liste-auf-gestohlenem-band-1.18208255). Hackers gained access to the Schengen Information System SIS database and were able to copy 1.2 million records. The attack was on an IT systems service provider in Denmark, which at the time was responsible for Denmark's copy of the Schengen database, among other things. (http://www.spiegel.de/netzwelt/netzpolitik/sis-hacker-kopierten-teile-der-schengen-datenbank-a-944059.html). The fact that the providers mentioned, including Swisscom, cannot consistently guarantee data security indicates that there is a fundamental problem here. The state is asking private providers to collect data without guaranteeing the security of the recorded data. This is another aspect that makes the encroachment on fundamental rights appear serious. The fundamental rights affected and, in particular, the secrecy of telecommunications are not safeguarded in this way (see Decision No. 1258 of the Romanian Constitutional Court).

92. This has recently been underscored by the large number of (successful) cyberattacks from which Swiss authorities and Swiss providers have also suffered. This has recently also affected the federal authorities to a large extent, which is why the Federal Council felt compelled to mandate a political-strategic crisis team «Datenabfluss» («Data Leakage») (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-96169.html).

93. The lack of data security and the lack of purpose limitation of the data involve a further risk: if data must be stored, but its data security is not guaranteed, this can also lead to the data being misappropriated with any other intentions. Among other things, the data can also be used to compromise or blackmail data subjects. Examples from the U.S. intelligence community show that this is not just a theoretical risk, but a real one (cf. http://www.thedailybeast.com/articles/2011/08/02/fbi-director-hoover-s-dirty-files-excerpt-from-ronald-kessler-s-the-secrets-of-the-fbi.html; https://www.aclu.org/blog/national-security-technology-and-liberty/prospect-blackmail-nsa).

94. All the events that have become known in connection with the NSA and other services (see http://www.theguardian.com/world/edward-snowden) also show that the risk of misappropriation of data is real and considerable

H. Access to retained data

95. As stated, access to the retained data is not limited to the prosecution of serious or most serious crime, and the protection of professional secrets and journalistic source protection are not sufficiently guaranteed.

96. As explained, the law also allows the use of metadata for the prosecution of minor crimes. The law has a precedent-setting effect on practice by also declaring the use of the metadata for minor crime to be permissible. The claim that in practice it is effectively verified whether the use of the metadata by the authorities is justified and that the courts and authorities involved in the decision ensure that no use of the stored metadata is possible that violates fundamental rights is as stated inaccurate and fails to take into account the practice as it is implemented in reality.

97. In particular, it is not true that the state attorney and the courts effectively implement the principle of subsidiarity. For example, it is common practice that surveillance measures are taken by default for certain offenses, including the use of retained data, without it having been demonstrated by the investigating authorities or investigated by the court, as provided for in the law (esp. Art. 269 para. c CCP), whether the investigative actions taken to date have been unsuccessful or whether the investigations would otherwise be futile or disproportionately impeded. Since the practice of the courts regarding the approval of surveillance measures is not published and, in particular, is not tangible with regard to the conditions under which the courts approve surveillance measures in reality, it will be necessary for this to be examined in greater depth by the Court in the context of case. In any case, it is in line with the experience of the legal representative of the applicants as a criminal defense lawyer that the principle of subsidiarity is not effectively reviewed and not complied with in practice.

98. Furthermore, concerning the legal protection against the use of the data there are, as set out, systematic gaps.

99. The intelligence service's access to retained data is not sufficiently precise and effectively limited . According to the IntelSA, this is possible within the framework of procurement measures requiring approval (Art. 26 para. 1 lit. a IntelSA). The prerequisite is that there is a concrete threat within the meaning of Article 19 paragraph 2 letters a - d IntelSA (terrorism, prohibited intelligence service, proliferation or attack on a critical infrastructure) or that the protection of other important national interests according to Article 3 IntelSA requires this. These requirements are extremely vague. In particular, there are no precise requirements for the invocation of important national interests under Art. 3 IntelSA. While there must be a serious and immediate threat, the interests that must be affected are very vague and broadly formulated. If the intelligence service claims that a concrete threat or the protection of other important national interests according to Art. 3 IntelSA requires the use of surveillance data, the court, which has to approve the measure, will not be able to verify whether the insinuated threat and the

relevance of the person affected by the surveillance are given in this respect or not. The court will only be able to verify whether the intelligence service makes allegations that meet the legal requirements. The person concerned will not find out about this and will regularly not be informed about the measure, even afterwards. Every person affected by data retention thus runs the risk of becoming the target of such a measure requiring approval without there being any suspicion of a criminal act, and any assumptions made by the intelligence service that make the person the target of the measure need by no means be accurate, so that the person concerned may become the target of the measure without having given concrete cause for it. Moreover, since the intelligence service can disclose personal data or lists of personal data abroad pursuant to Art. 61 IntelSA, compliance with fundamental rights is even less guaranteed in the case of data retained by the intelligence service.

I. Time limit for data retention

100. Like the ECJ, the applicants are of the opinion that it is not the specific duration of retention that is the central problem, but the indiscriminate retention of the metadata itself. Outside of the narrowly defined exceptions as set forth by the ECJ, or beyond an approach such as «quick freeze», the use of metadata does not appear to be justified.

J. Removal of monitoring and destruction of data

101. As explained, a very large amount of data accumulates at the providers. The destruction of all this data is not guaranteed in reality.

102. Even the law enforcement authorities will not be able to guarantee that the data will in reality be consistently destroyed as outlined by the government, not least because the authorities process a large volume of such data and the data will be available in different places at the same time, as explained below. The federal structure of law enforcement agencies and police in Switzerland must also be taken into account. In addition to the Attorney General of Switzerland and the Federal Police, each canton has several public prosecutor's offices, and in some cantons not only the cantonal police are involved in criminal proceedings, but also the independently organized police of larger cities.

104. The possibility of demanding the destruction of data in accordance with the provisions of the Data Protection Act does not provide any remedy in reality, if only because the person concerned cannot obtain an overview of where the data are stored everywhere. If the data is used in criminal proceedings or

by the intelligence service, it will in any case be stored in several data systems simultaneously.

III. Art. 10 of the Convention

105. The Government argues that the applicants suffer no direct consequences as a result of the providers' retention of their metadata, and it also denies that the retention of metadata has a chilling effect. Neither is true. Contrary to the government's view, there is indeed an interference with the freedom of expression.

106. The data stored allow conclusions to be drawn about who the applicants communicate with and how often, about their behavior and their personal and political views, and conclusions can also be drawn about the content of the communication, even more so if it is combined with other data.

107. The mere possibility that communications information is collected creates an infringement of privacy and a potential chilling effect on the rights concerned, including the right to freedom of expression. This infringement exists by the very fact of the retention of the metadata itself, and is substantially aggravated by the possibility that the data may be requested and used by public authorities. This is in itself an interference with the right to freedom of expression.

108. However, the interference is not limited to the «chilling effect» described above, but also consists directly in the fact that data of the applicants about whom they communicate with, where they are while doing so are stored by the providers. As explained, this data can be used to draw a variety of conclusions about their communication behavior. In this respect, the storage of the metadata associated with their communication constitutes an encroachment on their right to freedom of expression. The right to freedom of expression includes being able to communicate freely from the fact that such data associated with the communication, which as explained above allow further conclusions to be drawn about their communication, are recorded. If the corresponding data is then transmitted to law enforcement agencies or to the intelligence service, which cannot be foreseen and is explained to the applicants elsewhere, this constitutes a further encroachment on the right to freedom of expression, because the relevant authority then also obtains knowledge of the metadata and can draw the relevant conclusions about the communication behavior of the applicants.

109. It must be remembered that journalistic protection of sources derives in particular from Art. 10 of the Convention. It violates the right to journalistic source protection if metadata relating to the communication between the

journalist and his source are stored and can be disclosed to the authorities. The fact that the journalist and his source are not informed when the metadata concerning them are disclosed to an authority and have no effective means of appeal against this contributes to and aggravates the violation. Thus, the challenged retention of metadata has a chilling effect on communication between journalists and their sources and thus jeopardizes journalistic activity as an essential component of democracy.

110. Whether there is an encroachment on the freedom of opinion and in particular on the right to journalistic protection of sources must be examined comprehensively, as explained, also with regard to the fact that the data stored by the provider may be transmitted to the authorities. In this context, as explained, it must be taken into account that the protection of the right to source protection can no longer be guaranteed and that a violation of this right cannot be reversed once the authorities have received the data relating to communications between a journalist and his or her source.

102. All applicants are, moreover, specifically dependent on being able to communicate free of surveillance and are therefore particularly affected by the chilling effect associated with the metadata of their communications being retained by the providers:

103. G. is a member of the National Council, former parliamentary group president and now party president of the Green Party of Switzerland. Privately and politically, he is concerned with surveillance in the public and digital space and advocates for freedom of expression and unhindered access to information. In addition, as a board member of the association solidarité sans frontières, he is committed to, among other things, the exercise of the fundamental rights of Sans-Papiers, asylum seekers and other migrants and is a board member of the Tenants' Association of Switzerland (see https://www.balthasar-glaettli.ch).

104. In his function as a member of the National Council, but also due to his involvement in the above-mentioned cases, he repeatedly communicates with lawyers in order to obtain expert legal advice for himself and for third parties in individual factual matters. In doing so, he would actually be dependent on being able to benefit from the attorney-client privilege. However, this is partially undermined by data retention.

105. As a national parliamentarian, he also repeatedly receives confidential information from the population via e-mail and telephone. In order to clarify the facts, he in turn also contacts the persons concerned via the aforementioned channels and, if necessary, arranges contacts with media representatives or contacts them directly. In these sensitive cases in

particular, data retention not only undermines the protection of privacy and the secrecy of correspondence, mail and telecommunications of both communication partners, but as a consequence also undermines the protection of journalistic sources.

106. A technically possible, encrypted and, above all, obfuscated communication, which in particular does not generate any analyzable boundary data, for example, requires considerable technical knowledge on the part of all communication partners. The usual encryption technologies in particular encrypt the content of the communication, but do not disguise the edge data of the communication. Despite certain technical possibilities, data retention thus generates corresponding data relating to G., and his communication behavior is impaired.

107. M. is an activist of the Chaos Computer Club Zurich CCCZH and the Chaos Computer Club Switzerland CCC-CH. As an academic and as an activist, he is active in various professional networks and in protest networks.

108. Again and again, he has to deal with people who move on the outer left fringe of society and are active in projects that are in legal gray areas, such as the «Autonomer Beauty Salon ABS» or the «Autonome Schule Zürich ASZ». Due to his activities at neuralgic points of net as well as left politics, he assumes to be in a significant position in many communication networks, as they can be seen from the data retention.

109. The complainant wrote his master's thesis at the Institute for Computational Linguistics at the University of Zurich on the topic of «Computerlinguistik und Massenüberwachung» «Computational Linguistics and Mass Surveillance» (archive.org/details/MA_computerlinguistikmassenueberwachung). During his studies, he was affected by the use of the «pornography filter» temporarily deployed by the university (http://www.nzz.ch/digital/universitaet-zuerich-schaltet-pornofilter-vorerst-ab-1.18265443), and his university e-mail account was covered by the data deliveries to the public prosecutor's office in the course of the «Mörgeli affair», in which telephone contacts via university connections were then also evaluated. This involved media contacts, whereby he was targeted because (in a completely different context) email correspondence had been conducted «Tages-Anzeiger» (cf. on the «Mörgeli affair» and the Ritzmann case 1B_26/2016 as well as GYÖRFFY, loc. cit., para. 28 et seq.).

110. given its intention to give a voice to oppressed minorities and to provide society as a whole with greater transparency and democratic control over

social institutions, the complainant considers its activities to be legitimate and worthy of protection.

111. due to his knowledge of data retention and in particular the awareness that third parties can also always become the subject of "retroactive surveillance" made possible by data retention, he is too often confronted with the situation of deliberately not using the cell phone or only using it to a limited extent, deliberately switching it on, switching it off, deliberately leaving it at home or laying false tracks.

112. The user tries to prevent the surveillance measures as far as possible. However, this is only possible to a limited extent and, due to data retention, he can only use the wide range of electronic communication options with severe restrictions. Overall, his communication is significantly restricted by data retention.

113. He knows that this «surveillance pressure» not only for him, but also for many other activists with an awareness of data retention leads them to see their freedom of expression as well as their freedom of assembly restricted, which altogether disturbs democratic participation on all channels.

114. He is convinced that it cannot be the task of a progressive society to prevent committed people from expanding the liberal structures of the same: He is therefore in favor of abolishing data retention in Switzerland as well.

115. S. is a computer scientist and telecommunications specialist with in-depth knowledge of IT security. He is the managing director of the Digitale Gesellschaft, which he co-initiated (https://www.digitale-gesellschaft.ch/uber-uns/kurzvorstellung-personen/). He is interested in the area of conflict between technology, society and law. In his private life, he also deals with surveillance in the public and digital spheres and is committed to freedom of expression and unhindered access to information.

116. As stated by the German Federal Constitutional Court in its ruling on the retention of data, the storage of telecommunications traffic data without any reason is likely to give rise to a diffuse, threatening feeling of being watched, which can impair the unbiased exercise of fundamental rights in many areas.

117. The knowledge of data retention thus influences personal communication and participation in public life. For some time now, he has been surfing exclusively via proxy servers, often leaves his cell phone switched off or at home, and owns a not-so-smart smartphone instead of a modern one.

118. This reveals two possible reactions: Those who know how to help themselves technically (and have the corresponding resources available) avoid possible surveillance measures. From a broader perspective, this can lead to a situation in which comprehensive and suspicion-independent data retention ultimately results in less information being available for uncovering serious crime, as corresponding defensive measures are taken. Which, in the logic of the surveillance authorities, may well lead to even more far-reaching measures. Those who are unable to escape surveillance are more likely to restrict their communication behavior and freedom of movement. Freedom of expression, freedom of assembly, and ultimately participation in democratic processes are impaired.

119. However, it is precisely these principles that a free, democratic society must guarantee. This is what fundamental rights stand for. Data retention fundamentally conflicts with these freedoms.

120. S. tries to help himself against the surveillance measures as much as possible. However, this is only possible to a limited extent, and he can only use the manifold possibilities of electronic communication with weighty restrictions due to the data retention. Overall, his communication is significantly restricted by data retention.

121. St. has a focus on research in his journalistic work, which he carries out mainly as editor-in-chief of "Beobachter," a magazine that deals in particular with the law and its effect on individuals and society, the protection of consumers, and the exposure of misconduct by the state and business (https://...). Among other things, he regularly publishes critical articles on the judiciary in Switzerland (https://...). In his journalistic work, he is essentially dependent on the protection of his journalistic sources being guaranteed.

122. H. is a journalist, artist and politician (https://...). He was a long-time member of the municipal council of the city of St. Gallen and the cantonal council of St. Gallen and continues to be politically active. In all these activities it is of eminent importance for him to be able to communicate unsupervised. As a parliamentarian and politically engaged person, he is always in contact with the population, receives various information and establishes contacts. Data retention undermines the protection of privacy and the secrecy of correspondence, mail and telecommunications of both communication partners, especially in these sensitive cases. In his journalistic work, he is essentially dependent on the protection of his journalistic sources being guaranteed.

123. B. is actively involved in the international discourse on Internet governance issues from a civil society perspective. On some of these issues, there is a direct conflict of interest between this civil society perspective and the particular interests of certain U.S.-based companies. In the policy discourses in question, the number of individuals friendly to U.S. business interests is very large, and coordination among these individuals also tends to work well and be effective. This makes it all the more important for representatives of other civil society perspectives to also be able to communicate with each other and exchange documents without the risk of potentially being spied on in the process. From his perspective, it is therefore particularly important that the fundamental rights affected by data retention are safeguarded.

124. He regularly attends international conferences such as the United Nations Internet Governance Forum (IGF), occasionally using the provider's cell phone service to communicate with people with whom he also exchanges documents that would be of interest to political opponents. Now, he has IT expertise that allows him to protect his computers relatively well from unauthorized access. The computers of many communication partners are much less well protected.

125. Data retention without adequate precautions to protect communications edge data from unauthorized access means that an attacker who gains access to this communications edge data will know which relatively poorly protected computers could be broken into in order to gain access to the content of the abrogator's communications.

126. Furthermore, in these political contexts, the communication edge data itself, which shows who communicates with whom, is particularly worthy of protection, insofar as it is extremely unfair and represents a power factor if one side in political disputes has insight into the communication habits of the other side.

127. B. relies on reasonable special precautions to protect communications edge data from unauthorized access.

128. Thus, all applicants are in a situation where they are concretely affected by the storage of metadata. All applicants conduct very sensitive communications in their professional activities and in their private activities. It is of great importance to them that no conclusions can be drawn about their communication behavior from the data stored by the providers. All applicants are therefore forced to adapt their communication behavior by avoiding, wherever possible, communication channels where metadata is generated and stored by providers. This affects their communication and their communication options. In their professional and private

communications, they are contacted by other people who may not be as careful, either due to a lack of technical knowledge or due to a lack of technical alternatives, to avoid metadata in their communications that are stored by the providers. As shown above, these are, among others, other persons who share particularly sensitive communication content or who are themselves in a sensitive and exposed position (in particular Sans-Papiers, asylum seekers and other migrants, persons seeking legal advice or legal representation, who represent a political concern and wish to contact a member of parliament, political activists who wish to exchange views with other persons, and journalistic sources). If the applicants are contacted by such persons via the usual electronic communication channels and the resulting metadata are stored by the providers, then the providers and, if the data are released to the authorities, the authorities have data that allow conclusions to be drawn about the communication between the applicants and their communication partners. As explained, this is an interference with their right to freedom of expression, which includes communication with other persons and the possibility of receiving information from other persons.

129. In their activities, the applicants are also specifically dependent on being able to obtain information via electronic channels, in particular on the Internet, and to disseminate information via these channels (right to informational self-determination as a component of the right to freedom of expression).
With regard to this communication as well, in particular with regard to obtaining communication from the Internet, it is possible to draw conclusions about their communication behavior from accruing metadata, in particular about what they inform themselves about.

130. There are studies which prove that it generally has an effect on the use of communication options via electronic channels and in particular on the procurement of information via the Internet if people are aware that they can expect that their communication behavior can be recorded and the corresponding data can be evaluated by the authorities.

131. An empirical study carried out by Jonathon W. Penney provides evidence of regulatory chilling effects of Wikipedia users associated with online government surveillance (DOI: https://doi.org/10.15779/Z38SS13). The article finds a statistically significant immediate decline in traffic for Wikipedia articles after the mass surveillance revelations on June 2013, and also a change in the overall secular trend in the view count traffic, suggesting not only immediate but also long-term chilling effects resulting from the NSA/PRISM online surveillance revelations.

132. Simon Assion demonstrates in his article «Überwachung und Chilling Effects» that the danger of chilling effects through surveillance can not only be justified theoretically, but can also be proven by concrete examples. For example, intimidation effects among Muslims when mass surveillance became known are demonstrable, as is the fact that after the NSA mass surveillance became known, users of Google were significantly less likely to search for search terms they considered «dangerous», that such self-restrictions affected, among others, writers, journalists, and translators who are members of PEN America, a significant number of whom subsequently avoided communicating on the phone or via email about certain topics, avoided writing about certain topics or at least seriously considered doing so and avoided researching certain topics online or at least seriously considered doing so (SIMON ASSION, Überwachung und Chilling Effect, in: «Überwachung und Recht», Tagungsband zur Telemediucs Sommerkonferenz 2014 [https://www.researchgate.net/publication/277711520_Uberwachung_und_Chilling_Effects]).

133. The impairment of the use of communication options via electronic channels and, in particular, the procurement of information via the Internet also affects the applicants, who, out of the fear that the procurement of information will lead to the collection of metadata related to it, adapt their behavior in the procurement of information and limit themselves in the procurement of information. The applicants actually do not use the information available on the Internet, including the use of messenger services and comparable communication platforms, without restriction and not without excessive caution, because they want to avoid providers and possibly authorities being able to draw conclusions from stored metadata as to where the applicants obtain information, especially since it often concerns political content and discussions.

134. As explained above, St. and H. are particularly affected by the risk of metadata being recorded by providers in connection with their professional activities and possibly used by the authorities. This also affects their research activities via electronic communication and on the Internet. It is particularly serious that the providers can collect metadata that show that they are in contact with journalistic sources and that this metadata could come to the attention of the authorities. As explained, this violates the right to journalistic source protection. As explained, the mere fact that a journalist communicates with his or her source is already subject to journalistic source protection. Authorities may not gain knowledge of who a journalist's source is. If a potential journalistic source risks being recorded and reconstructed as having contacted a journalist, then the source may refrain from contacting and communicating with the journalist. This severely compromises

journalistic source protection. St. and H. are concretely affected by all this in their work as journalists. They risk losing potential sources and cannot be sure that the protection of their sources against providers and authorities is working effectively.

IV. Art. 11 of the Convention

135. For the interference with Art. 11 of the Convention, essentially the same applies as has been explained with regard to Art. 10 of the Convention. From such metadata, far-reaching conclusions can be drawn about the applicants, in particular about whom they communicate with and how often, where they stay and where they go, and – especially in combination with data available about them from other sources, but also with other general data – about their behavior and their personal and political views. This can particularly affect communications before, during and after the conduct of peaceful assemblies.

136. The mere possibility that communications information is collected creates an invasion of privacy and a potential chilling effect on the rights at stake, including the right to freely and peacefully assemble. This infringement exists by the very fact of the retention of the metadata itself and is substantially aggravated by the possibility that the data may be requested and used by public authorities.

137. Moreover, the interference with Art. 11 of the Convention goes beyond the chilling effect. If the applicants participate in the organization of a peaceful assembly or merely consult with others about participation, and even if they participate in a peaceful assembly, indications of this may arise from the metadata of their communications. The fact that their metadata contains corresponding information constitutes an interference with their right to peacefully assemble with others. As with the interference with the right to private life and the right to freedom of expression, this interference is not justified.

V. Conclusions

138. The application is well-founded and, contrary to the arguments put forward by the government, Art. 8, Art. 10, Art. 11 as well as Art. 13 of the Convention are violated.

139. The applicants' request, made in the national proceedings, that the providers be ordered not to forward the traffic and billing data concerning them to the service or other authorities or courts should have been dealt with in the national proceedings. The request was well-founded and the applicants have

sufficiently addressed the contested decisions in their legal briefs with respect to this request. The PTSS and the courts would have been authorized to handle this request. Addressing this request was necessary to protect the applicants from the possibility that metadata stored at the providers concerning them could be disclosed to authorities or courts, which would have meant an additional violation of their fundamental rights.

140. Irrespective of how this request is dealt with, it should be noted that, in order to examine the compatibility of data retention with the providers, it is necessarily necessary to examine both what encroachment on fundamental rights they suffer as a result of the retention itself and what encroachment is associated with a use of the data by the authorities. There are two reasons for this: First, the purpose of the regulations on the retention of metadata by providers is nothing other than to keep this metadata available to the authorities. Thus, the retention and use of the data cannot be assessed separately. Since the purpose of storing the data is its use by the authorities, it must be comprehensively examined which encroachments on fundamental rights are or may be associated with data retention. This also includes use of the data by the authorities. How serious the encroachment on fundamental rights by data retention is, and whether this encroachment is justified, is also determined by how and under what conditions these data can ultimately be used by the authorities. Second, the encroachments on fundamental rights that result from the use of the data by the authorities are irreversible, and in various constellations there is no sufficient legal protection against the use of the data by the authorities after the metadata have been transmitted by the providers to the authorities. These gaps in legal protection after transmission to the authorities mean that effective legal protection must already be guaranteed at the stage of storage by the providers. This leads to the conclusion that in the case of insufficient protection against infringement through use by the authorities after transmission, the storage must already be prevented and the transmission of already stored data must be prevented in order to guarantee a right to effective protection of fundamental rights and to effective remedy in accordance with Art. 13 of the Convention. This applies to a greater extent to journalists and their sources, who are dependent on the fact that no conclusions can be drawn from stored metadata of their communications about the contact between journalists and sources in order to protect their claim.

142. The applicants have shown that the retention of the metadata and the use of this data by the authorities as provided for by law leads to serious interference with their fundamental rights protected in Art. 8, Art. 10 and Art. 11 of the Convention .

143. The applicants have also shown that data retention is not based on a sufficient and sufficiently concrete legal basis that is comprehensible to those subject to the law.

144. Further, the applicants have shown that the purposes invoked by the government cannot justify data retention.

145. Data retention does not appear to be necessary and proportionate to achieve the purposes pursued.

146. The applicants are affected by an general and indiscriminate retention of metadata of practically all individuals. The stored metadata may contain information about a variety of aspects of the private life of the data subjects, including sensitive information such as sexual orientation, political opinions, religious, philosophical, social or other beliefs, and health status. From the totality of these data, it is possible to draw very precise conclusions about the private life of the persons whose data have been stored, such as habits of daily life, permanent or temporary places of residence, daily or other rhythmic changes of place, activities carried out, social relations of these persons and the social environment in which they socialize. These data allow, in particular, the creation of a profile of the persons concerned, which is information as sensitive as the content of the communications themselves, with regard to the right to respect for private life. The storage and use of such metadata, as provided for by the law, cannot be justified for achieving the purposes pursued.

147. The requirements for the use of data in criminal proceedings are too low. They are not limited to the prosecution of serious or most serious crime, but according to the law and practice in Switzerland are already permitted for the prosecution of crime of relatively minor severity. This is clearly not sufficient to justify such an unprovoked data retention.

148. The conditions for the use of the data by the intelligence service are too imprecise and, in the final analysis, also too low to justify such an unprovoked retention of data.

149. The applicants' right to respect for private life and also their right to freedom of expression and peaceful assembly are impaired. This results from a chilling effect in that the applicants are under pressure to adapt and restrict their communication behavior due to the fact that the use of certain forms of communication generates metadata. However, even apart from the chilling effect, the storage and possible use of the metadata directly impairs their fundamental rights.

150. The impairment of the right is particularly serious in the case of St. and H. who are journalists. They depend on being able to be in contact with their sources and to inform themselves without metadata being created from which contacts with sources and their information behavior can be inferred.

151. The encroachments suffered by the applicants on their rights under Articles 8, 10 and 11 of the Convention are thus not justified. The national authorities, and in particular the Federal Court, have not adequately addressed these violations of the Convention and the applicants' arguments in this regard. In part, they have not even addressed the claims, and in part they have wrongly argued that they do not need to be addressed in these proceedings. Thus, the applicants' right to effective remedy under Article 13 of the Convention in combination with the rights under Articles 8, 10 and 11 of the Convention have been violated in the national proceedings .

152. The complaint must therefore be upheld. It has to be held that the applicants' rights under Articles 8, 10 and 11 of the Convention, and in combination therewith their claim under Article 13 of the Convention, have been violated as alleged by the the applicants. The Federal Supreme Court is to be obliged to revise its judgment, to also establish these violations and to ensure that the storage and use of metadata concerning the applicants, as provided for by law, is refrained from.

VI. Just satisfaction

153. The applicants instructed the undersigned lawyer to represent him in the proceedings before PTSS and the domestic courts. They have undertaken to reimburse the lawyer for the costs incurred with a fee based on time expenditure of CHF 220.00 per hour plus cash expenses and 8% (until 31.12.2017) or 7.7% VAT (from 1.1.2018). The attorney's time required for the domestic proceedings amounts to 68 h and 45 min, the cash expenses amount to CHF 267.95. The time required for the proceedings before the European Court of Human Rights so far amounts to 60 h and 40 min, the cash expenses amount to CHF 180.30. An estimated additional 15 hours is to be expected for the further proceedings. This amounts to a fee of 33'990.00 (154 hours 30 minutes à CHF 220.00 plus cash expenses), plus 8%/7.7% VAT in the amount of CHF 2'697.70. The total fee thus amounts to CHF 37'135.95. According to the current exchange rate (1 CHF = 1.024 ◘) this corresponds to ◘ 38'027.21. The statement of attorney's expenses is submitted together with the observations.

VII. Third-Party Submission made by the Estonian Government

154. Ad. 3.: The metadata are so closely linked to the communication itself that it cannot be said that data retention would not interfere with the right to secrecy of communication.

155. Ad. 4.: As explained above, there is a chilling effect with regard to the rights under Art. 10 and Art. 11 of the Convention. Moreover, the interference with these Convention rights is not limited to the occurrence of a chilling effect.

156. Ad. 5.: Insofar as Estonia emphasizes the importance of the review of proportionality, this is in principle to be agreed with. As explained above, proportionality must be assessed from a holistic perspective, which also includes the use of the data by the authorities.

157. Ad. 7. - 11.: It cannot seriously be said that the obligations of states in connection with the right to privacy could not be upheld without data retention. As explained, there are sufficient other approaches to meet these obligations. It should be pointed out once again that a number of states that are members of the Council of Europe do not practice data retention and can still fulfill their obligations under Article 8 of the Convention. The same applies to the obligation to combat the phenomena Estland refers to in para 8. - 11. Combating these phenomena cannot justify the storage of metadata without any reason to the extent envisaged by Switzerland. Moreover, the use of retained data in Switzerland goes far beyond addressing the problems mentioned by Estonia.

158. Ad. 13: The factors proposed by Estonia cannot, as is clear from the complainants' submissions, lead to the retention of data being considered to be in conformity with the rights of the Convention.

159. Ad.14 and 15: The seriousness of the interference with fundamental rights is greatly underestimated by Estonia. In particular, Estonia overlooks the fact that data retention cannot guarantee the protection of journalistic sources.

Best Regards,

Viktor Györffy

Enclosure: Statement of attorney's expenses