EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

ENG - 2016/1

Application Form

About this application form

This form is a formal legal document and may affect your rights and obligations. Please follow the instructions given in the "Notes for filling in the application form". Make sure you fill in all the fields applicable to your situation and provide all relevant documents.

Warning: If your application is incomplete, it will not be accepted (see Rule 47 of the Rules of Court). Please note in particular that Rule 47 § 2 (a) requires that a concise statement of facts, complaints and information about compliance with the admissibility criteria MUST be on the relevant parts of the application form itself. The completed form should enable the Court to determine the nature and scope of the application without recourse to any other submissions.

Barcode label

If you have already received a sheet of barcode labels from the European Court of Human Rights, please place one barcode label in the box below.

Reference number

If you already have a reference number from the Court in relation to these complaints, please indicate it in the box below.

A. The applicant

A.1. Individual

This section refers to applicants who are individual persons only. If the applicant is an organisation, please go to section A.2.

1. Surname

2. First name(s)

3. Date of birth

0	4	0	9	1	9	6	6
D	D	M	M	Y	Y	Y	Y

e.g. 31/12/1960

4. Place of birth

5. Nationality

Swiss

6. Address

7. Telephone (including international dialling code)

8. Email (if any)

9. Sex ◉ male ○ female

A.2. Organisation

This section should only be filled in where the applicant is a company, NGO, association or other legal entity. In this case, please also fill in section D.1.

10. Name

11. Identification number (if any)

12. Date of registration or incorporation (if any)

D	D	M	M	Y	Y	Y	Y

e.g. 27/09/2012

13. Activity

14. Registered address

15. Telephone (including international dialling code)

16. Email

B. State(s) against which the application is directed

17. Tick the name(s) of the State(s) against which the application is directed

- [ ] ALB - Albania
- [ ] AND - Andorra
- [ ] ARM - Armenia
- [ ] AUT - Austria
- [ ] AZE - Azerbaijan
- [ ] BEL - Belgium
- [ ] BGR - Bulgaria
- [ ] BIH - Bosnia and Herzegovina
- [x] CHE - Switzerland
- [ ] CYP - Cyprus
- [ ] CZE - Czech Republic
- [ ] DEU - Germany
- [ ] DNK - Denmark
- [ ] ESP - Spain
- [ ] EST - Estonia
- [ ] FIN - Finland
- [ ] FRA - France
- [ ] GBR - United Kingdom
- [ ] GEO - Georgia
- [ ] GRC - Greece
- [ ] HRV - Croatia
- [ ] HUN - Hungary
- [ ] IRL - Ireland
- [ ] ISL - Iceland
- [ ] ITA - Italy
- [ ] LIE - Liechtenstein
- [ ] LTU - Lithuania
- [ ] LUX - Luxembourg
- [ ] LVA - Latvia
- [ ] MCO - Monaco
- [ ] MDA - Republic of Moldova
- [ ] MKD - "The former Yugoslav Republic of Macedonia"
- [ ] MLT - Malta
- [ ] MNE - Montenegro
- [ ] NLD - Netherlands
- [ ] NOR - Norway
- [ ] POL - Poland
- [ ] PRT - Portugal
- [ ] ROU - Romania
- [ ] RUS - Russian Federation
- [ ] SMR - San Marino
- [ ] SRB - Serbia
- [ ] SVK - Slovak Republic
- [ ] SVN - Slovenia
- [ ] SWE - Sweden
- [ ] TUR - Turkey
- [ ] UKR - Ukraine

C. Representative(s) of the individual applicant

An individual applicant does not have to be represented by a lawyer at this stage. If the applicant is not represented please go to section E.

Where the application is lodged on behalf of an individual applicant by a non-lawyer (e.g. a relative, friend or guardian), the non-lawyer must fill in section C.1; if it is lodged by a lawyer, the lawyer must fill in section C.2. In both situations section C.3 must be completed.

C.1. Non-lawyer

18. Capacity/relationship/function

19. Surname

20. First name(s)

21. Nationality

22. Address

23. Telephone (including international dialling code)

24. Fax

25. Email

C.2. Lawyer

26. Surname
Györffy

27. First name(s)
Viktor

28. Nationality
Switzerland

29. Address
PSG-Rechtsanwälte
Beethovenstrasse 47
8002 Zürich

30. Telephone (including international dialling code)
+41 44 240 20 55

31. Fax
+41 43 500 55 71

32. Email
gyoerffy@psg-law.ch

C.3. Authority

The applicant must authorise any representative to act on his or her behalf by signing the first box below; the designated representative must indicate his or her acceptance by signing the second box below.

I hereby authorise the person indicated above to represent me in the proceedings before the European Court of Human Rights concerning my application lodged under Article 34 of the Convention.

33. Signature of applicant

34. Date
30/04/2018 e.g. 27/09/2015
D D M M Y Y Y Y

I hereby agree to represent the applicant in the proceedings before the European Court of Human Rights concerning the application lodged under Article 34 of the Convention.

35. Signature of representative

36. Date
27/09/2018 e.g. 27/09/2015
D D M M Y Y Y Y

D. Representative(s) of the applicant organisation

Where the applicant is an organisation, it must be represented before the Court by a person entitled to act on its behalf and in its name (e.g. a duly authorised director or official). The details of the representative must be set out in section D.1.

If the representative instructs a lawyer to plead on behalf of the organisation, both D.2 and D.3 must be completed.

D.1. Organisation official

37. Capacity/relationship/function (please provide proof)

38. Surname

39. First name(s)

40. Nationality

41. Address

42. Telephone (including international dialling code)

43. Fax

44. Email

D.2. Lawyer

45. Surname

46. First name(s)

47. Nationality

48. Address

49. Telephone (including international dialling code)

50. Fax

51. Email

D.3. Authority

The representative of the applicant organisation must authorise any lawyer to act on its behalf by signing the first box below; the lawyer must indicate his or her acceptance by signing the second box below.

I hereby authorise the person indicated in section D.2 above to represent the organisation in the proceedings before the European Court of Human Rights concerning the application lodged under Article 34 of the Convention.

52. Signature of organisation official

53. Date

e.g. 27/09/2015

D D M M Y Y Y Y

I hereby agree to represent the organisation in the proceedings before the European Court of Human Rights concerning the application lodged under Article 34 of the Convention.

54. Signature of lawyer

55. Date

e.g. 27/09/2015

D D M M Y Y Y Y

Subject matter of the application

All the information concerning the facts, complaints and compliance with the requirements of exhaustion of domestic remedies and the six-month time-limit laid down in Article 35 § 1 of the Convention must be set out in this part of the application form (sections E, F and G). It is not acceptable to leave these sections blank or simply to refer to attached sheets. See Rule 47 § 2 and the Practice Direction on the Institution of proceedings as well as the "Notes for filling in the application form".

E. Statement of the facts

56.
1. Der Beschwerdeführer ist Kunde der Swisscom AG (nachfolgend: Anbieterin).
2. Gemäss Art. 15 Abs. 3 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (nachfolgend: BÜPF) sind die Anbieterinnen von Fernmeldediensten verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten (nachfolgend: Metadaten) während sechs Monaten aufzubewahren (Vorratsdatenspeicherung). Die Anbieterin speichert demnach gestützt auf Art. 15 Abs. 3 BÜPF, d.h. gestützt auf öffentliches Recht des Bundes, während sechs Monaten die erwähnten Metadaten, die bei der Kommunikation der Beschwerdeführer anfallen.
3. Unter den in Art. 273 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (nachfolgend: StPO) genannten Voraussetzungen kann die Staatsanwaltschaft gespeicherte Vorratsdaten herausverlangen und als Beweismittel in der entsprechenden Strafuntersuchung verwenden. Art. 273 StPO verweist sodann auf die Voraussetzungen von Art. 269 Abs. 1 lit. b (genügende Schwere der Straftat) und c (Subsidiarität: Erfolglosigkeit der bisherigen Ermittlungen, Aussichtslosigkeit oder unverhältnismässige Erschwerung der Ermittlungen) StPO. Grundsätzlich reicht für die Nutzung der Vorratsdaten jeder dringende Verdacht auf ein Verbrechen (Taten, für die die Höchststrafe mehr als drei Jahre Freiheitsstrafe beträgt) oder Vergehen (Taten, für die eine Geldstrafe oder eine Freiheitsstrafe bis zu drei Jahren vorgesehen ist) aus, im Fall von Artikel 179septies StGB (Missbrauch einer Fernmeldeanlage) sogar der Verdacht auf eine Übertretung, welche lediglich mit einer Busse von maximal CHF 10'000.00 bestraft werden kann (Art. 103 i.V.m. Art. 106 StGB). Die Verwendung von Vorratsdaten beschränkt sich also grundsätzlich nicht auf Fälle schwerer Kriminalität, sondern erfasst gemäss der gesetzlichen Definition auch Delikte von verhältnismässig geringer Schwere. Die vorgesehene Nutzung ist nicht auf die Daten von verdächtigen Personen beschränkt, sondern erstreckt sich auch auf nicht verdächtigte Dritte.
4. Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin gemäss Art. 14 Abs. 4 BÜPF verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.
5. Die Herausgabe der Daten wird durch die Staatsanwaltschaft angeordnet (Art. 273 Abs. 1) und durch das Zwangsmassnahmengericht (nachträglich) genehmigt (Abs. 2). Der Dienst ÜPF überprüft ob eine Überwachungsanordnung eine überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet wurde. Sodann weist er die Anbieterin von Fernmeldediensten an, ihm die für die Überwachung notwendigen Daten zu übermitteln und leitet diese dann an die Strafverfolgungsbehörde weiter. (Art. 13 Abs. 1 BÜPF). Anbieterinnen eines Postdienstes leiten die Sendungen oder Informationen direkt an die anordnende Behörde (Art. 11 Abs. 1 lit. a BÜPF). Auch der inländische Nachrichtendienst (NDB) kann auf gewisse Vorratsdaten zugreifen (Daten gemäss Art. 14 Abs. 1 lit. a BÜPF i.V.m. Art. 14 2bis BÜPF).
6. Es werden systematisch Daten im Zusammenhang mit schriftlicher und mündlicher Kommunikation erfasst, insb. Daten aus der Kommunikation via Telefon, Mail, Internet und von Briefpostsendungen. Zu erfassen sind u.a. Grunddaten des Kunden, Telefonnummern der anrufenden Person und der Gegenseite, Angaben zum verwendeten Geräte und zur verwendeten Datenleitung sowie Standortdaten (insb. Mobilfunkantenne). Daraus lässt sich u.a. schliessen, wer mit wem wann kommuniziert und wo sich die involvierten Personen aufhalten.
7. Welche Daten von welchen Anbietern zu speichern sind, erschliesst sich nicht ohne Weiteres. Auf Gesetzesstufe (Gesetz im formellen Sinn) sind die Regelungen in der StPO und im BÜPF festgelegt. Aus dem Studium der entsprechenden Gesetzesartikel wird aber nicht klar, welche Daten von welchen Providern genau erfasst werden müssen. Dies ist lediglich in untergeordneten Verordnungen und Richtlinien geordnet. Den Rechtsunterworfenen ist damit in ganz wesentlichen Aspekten nicht klar, welche Daten überhaupt erfasst werden.
8. Über die Kanäle, die von der Vorratsdatenspeicherung tangiert sind, läuft sehr viel Kommunikation, und es fallen auch viele Standortdaten an. Die Vorratsdatenspeicherungsdaten sind sehr aussagekräftig, auch wenn dabei kein oder kaum Kommunikationsinhalt gespeichert wird.
9. Die Gerichtspraxis hat markante Ausweitungen der Vorratsdatenspeicherung auf Verordnungsstufe zugelassen, beispielsweise die Rasterfahndung in gespeicherten Antennenstandorten samt Hauptstrahlrichtung von Mobiltelefonen (sog. Antennensuchlauf), die Kopfschaltung, mit der die Vorratsdaten aller inländischen Telefonanschlüsse nach allfälliger Kommunikation mit einem bestimmten ausländischen Anschluss gerastert werden. Ebenfalls nicht dem Gesetz entnehmen lässt sich die Verpflichtung der Provider, je nach Technik des Internetzugangs nicht nur die IP-Adresse zu speichern, sondern auch NAT-Daten. Daraus lässt sich nicht nur rekonstruieren, welches Gerät welche IP und welche Ports benutzt hat, sondern es ist auch möglich, die vom entsprechenden Gerät besuchten Server nachvollziehen und ein umfangreiches Surfprofil erstellen.

Statement of the facts (continued)

57.
10. Die Vorratsdatenspeicherung verletzt eine Reihe von datenschutzrechtlichen Grundsätzen und bietet keine zureichenden Garantien zum Schutz vor Missbrauch bei der Bearbeitung von Personendaten.
11. Am 1. März 2018 trat das revidierte BÜPF (nachfolgend: nBÜPF) mitsamt überarbeiteter Verordnung (nVÜPF) in Kraft. Mit der Totalrevision wurde zwar der Inhalt der Vorratsdatenspeicherung weitgehend konkretisiert, aber wiederum nicht auf Gesetzes- sondern lediglich auf Verordnungsstufe.
12. Zudem wurde mit der neuen Gesetzgebung der persönliche Anwendungsbereich und damit der Kreis der Mitwirkungspflichtigen ausgeweitet (Art. 2 nBÜPF). Insbesondere müssen neu auch Anbieterinnen abgeleiteter Kommunikationsdienste die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs liefern und sie können zur Aufbewahrung der Randdaten für 6 Monate verpflichtet werden (Art. 27 Abs. 2 und 3 nBÜPF). Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen, sind zwar nicht zur Aufbewahrung von Randdaten verpflichtet, müssen die ihnen zur Verfügung stehenden Randdaten jedoch den Strafverfolgungsbehörden zur Verfügung stellen (Art. 29 Abs. 3 nBÜPF).
13. Auch der Anwendungsbereich des BÜPF wurde ausgeweitet (Art. 1 Abs. 1 lit. d und e.) Neu findet es auch Anwendung auf die Fahndung nach Personen, die zu einer Freiheitsstrafe verurteilt wurden oder gegen die eine freiheitsentziehende Massnahme angeordnet wurde. Weiter ist das nBÜPF auch im Rahmen des Vollzugs des neuen Nachrichtendienstgesetzes (NDG) anwendbar. So kann neu auch der Nachrichtendienst auf die Randdaten des Post- und Fernmeldeverkehrs zugreifen (Art. 26 Abs. 1 lit. a NDG). Dazu bedarf er zwar einer Genehmigung, die strafprozessualen Garantien und damit eine wirksame Beschwerdemöglichkeit entfallen dabei jedoch gänzlich, denn die Überwachung erfolgt geheim und betroffene Personen werden über die Verwendung der Daten nicht in Kenntnis gesetzt (Art. 26 Abs. 2 NDG). Insgesamt fallen im Rahmen des nBÜPF nochmals deutlich mehr Vorratsdaten an.
14. Die Vorratsdatenspeicherung gemäss der dargelegten Regelung erfasst auch die entsprechenden Metadaten im Verkehr zwischen Journalisten und ihren Kommunikationspartnern, einschliesslich ihrer Quellen. Es besteht keine Regelung, welche Journalisten von der Vorratsdatenspeicherung ausnimmt, so weit dies den journalistischen Quellenschutz betrifft. Zwar verankern Art 28a StGB und Art. 172 StPO den Quellenschutz und postulieren grundsätzlich die Straflosigkeit und ein Verbot strafprozessualer Zwangsmassnahmen für den Fall, dass ein Journalist als Zeuge seine Quelle nicht offen legt. Der so festgelegte Schutz der Medienfreiheit und der Quellenschutz erweist sich als ungenügend. Soweit das in Art. 28a StGB enthaltene Verbot von Zwangsmassnahmen greift, ist der Journalist zwar davor geschützt, dass die vorhandenen Metadaten durch Anordnung von Massnahmen gemäss Art. 273 StPO (Auskunft über Verkehr- und Rechnungsdaten Teilnehmeridentifikation) gegen den Journalisten an die Staatsanwaltschaft gelangen. Eine solche Massnahme ist damit unzulässig, soweit sie nur zum Ziel hat, den Quellenschutz zu unterlaufen (Hansjakob, Kommentar BÜPF/VÜPF, Art. 4 N 31 ff). Dies ändert aber nichts daran, dass die entsprechenden Metadaten, die in der Kommunikation mit Quellen anfallen, im Rahmen der Vorratsdatenspeicherung erfasst werden.
15. Art. 271 StPO verankert den Schutz von Berufsgeheimnissen i.S.v. Art. 271 StPO bei Überwachungen. Richtet sich die Überwachung gegen eine Person, die einer Berufsgruppe gemäss Art. 170 - 173 angehört, so sind Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, unter der Leitung eines Gerichts auszusondern. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen. Art. 271 Abs. 2 StPO schränkt die Zulässigkeit von Direktschaltungen ein in Fällen, in denen sich die Überwachung gegen Berufsgeheimnisträge richtet. Diese Vorschrift greift aber nicht, weil sie sich in der Praxis technisch nicht umsetzen lässt. Gemäss Art. 271 Abs. 3 sind bei der Überwachung anderer Personen Informationen, über welche eine in den Art. 170 - 173 genannte Person das Zeugnis verweigern könnte, aus den Verfahrensakten auszusondern und sofort zu vernichte; sie dürfen nicht verwendet werden. Effektiv lässt es sich bei Vorratsdaten aber nicht vermeiden, dass diese der Strafverfolgungsbehörde zur Kenntnis gelangen, bevor die Mechanismen, wie sie in Art. 271 StPO vorgesehen sind, greifen können.
16. Fatal für den Quellenschutz ist u.a. die Regelung, wonach die Staatsanwaltschaft die geheime Überwachung anordnet und das Zwangsmassnahmengericht erst nachträglich innert fünf Tagen über dessen Zulässigkeit entscheidet (Art. 274 StPO). Daten, die unmittelbar nach der Anordnung anfallen, sind für die Staatsanwaltschaft laufend einsehbar und können von dieser ausgewertet werden. Die Strafverfolgungsbehörden können nicht gleichzeitig die in Echtzeit hereinkommenden Daten für das laufende Strafverfahren nutzen und dieselben Daten, soweit sie dem Quellenschutz unterliegen, nicht zur Kenntnis nehmen. Tangieren die anfallenden Daten den Quellenschutz, ist dieser damit bereits durchbrochen (Györffy, a.a.O., Rz. 19 f.). Dies gilt auch für anfallende Vorratsdaten.
17. Aus Vorratsdaten, welche bei den Strafverfolgungsbehörden liegen, lassen sich Daten, welche vom Quellenschutz erfasst sind und von denen die Strafverfolgungsbehörden deshalb keine Kenntnis haben dürfen, nicht mehr effektiv aus den Akten aussondern, und die Durchbrechung des Quellenschutzes lässt sich regelmässig mehr nicht verhindern. Zu schützen ist insbesondere die Information, dass ein Journalist mit einer Quelle kommuniziert hat bzw. dass diese Person eine journalistische Quelle ist. Sobald die entsprechenden Daten den Strafverfolgungsbehörden vorliegen, haben sie

Statement of the facts (continued)

58.
unmittelbar Kenntnis von diesen Tatsachen. Und wenn sie nicht realisieren sollten, dass es sich um Informationen handelt, welche dem Quellenschutz unterliegen, lassen sich die Daten höchstens dann aus den Akten entfernen, wenn der Staatsanwalt, ein Gericht, der Journalist oder die Quelle Tatsachen realisiert oder vorbringt, welche belegen, dass Quellenschutz zu gewährleisten ist. Mit dem Bekanntwerden dieser Tatsachen wird der Quellenschutz aber gerade durchbrochen, da gerade auch diese Tatsachen – namentlich der Umstand, dass ein Journalist und seine Quelle kommunizieren bzw. wer die Quelle ist –dem Quellenschutz unterliegt. Ob der Journalist und/oder seine Quelle davon erfahren, dass den Strafverfolgungsbehörden Vorratsdaten, die dem Quellenschutz unterliegen, vorliegen, und ob sie so am Verfahren beteiligt werden, dass sie den Quellenschutz geltend machen können, steht zudem keineswegs fest. Die strafprozessualen Vorschriften, welche zur Gewährleistung des Quellenschutzes aufgestellt worden sind, vermögen den Quellenschutz damit nicht wirksam zu gewährleisten, auch nicht in Fällen, in denen keine zureichenden Gründe bestehen würden, um den Quellenschutz zu durchbrechen.
18. Der Beschwerdeführer hat in seiner journalistischen Tätigkeit einen Schwerpunkt im Bereich Recherche. Er publiziert u.a. regelmässig kritische Artikel zur Justiz in der Schweiz. Er ist in seiner journalistischen Tätigkeit essenziell darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist. Der Beschwerdeführer versucht, sich nach Möglichkeit gegen die Überwachungsmassnahmen zu behelfen. Dies geht jedoch nur eingeschränkt, er ist nicht frei in der Wahl der tauglichen Kommunikationsmittel (auch, weil sich der Beschwerdeführer Kommunikationskanäle mit anderen Personen erhalten muss) und kann die mannigfaltigen Möglichkeiten der elektronischen Kommunikation aufgrund der Vorratsdatenspeicherung nur mit deutlichen Einschränkungen nutzen. Aus den Vorratsdaten können Rückschlüsse auf die beruflichen Aktivitäten des Beschwerdeführers, seine Recherchen und seine Kontakte zu Drittpersonen gezogen werden. Vorratsdaten lassen Rückschlüsse darauf zu, mit welchen Personen er wann kommuniziert hat und wo sich die kommunizierenden Personen aufgehalten haben. Damit sind auch Schlüsse auf Kontakte mit journalistischen Quellen möglich.
Prozessgeschichte:
1. 20. Februar 2014, Gesuch an den Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend: Dienst ÜPF), die Swisscom AG sei anzuweisen, die gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten des Gesuchstellers zu löschen und deren Speicherung in Zukunft zu unterlassen, soweit die betroffenen Daten nicht für die Erbringung der vertraglichen Leistungen gegenüber dem Gesuchsteller zwingend erforderlich sind. Die Swisscom AG sei zudem anzuweisen bzw. zu verpflichten, keine gemäss Art. 15 Abs. 3 BÜPF gespeicherten Verkehrs- und Rechnungsdaten des Gesuchstellers an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben.
Das Gesuch wird damit begründet, dass Speicherung der Metadaten einen schweren und unrechtmässigen Eingriff in folgende Grundrechte darstellt: Die Unschuldsvermutung (Art. 6 EMRK), das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich die Achtung des Brief-, Post- und Fernmeldeverkehrs, das Recht auf Schutz vor Missbrauch der persönlichen Daten und auf informationelle Selbstbestimmung, sowie die persönliche Freiheit und die Bewegungsfreiheit (Art. 8 EMRK), die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit (Art. 10 EMRK), die Versammlungsfreiheit (Art. 11 EMRK), sowie das Recht auf eine effektive Beschwerde (Art. 13 EMRK).
2. 30. Juni 2014 Verfügung des Dienstes ÜPF: Auf das Begehren, der Swisscom AG sei die Herausgabe der Daten an Behörden zu verbieten, wird nicht eingetreten. Es mangle an einem schutzwürdigen Interesse, da die Möglichkeit zur Beschwerde im Nachhinein durch Art. 279 StPO geregelt sei, im Übrigen wird das Gesuch abgewiesen.
3. 2. September 2014, Beschwerde an das Bundesverwaltungsgericht mit im Wesentlichen denselben Anträgen wie im Gesuch an den Dienst ÜPF.
4. 9. November 2016, Urteil des Bundesverwaltungsgerichts: Die Beschwerde wird abgewiesen (nachdem das Gericht die Verfahren der 6 Beschwerdeführer vereinigt hatte). Der Dienst ÜPF sei zurecht nicht auf den Antrag eingetreten, der Anbieterin sei zu verbieten, Daten an Behörden herauszugeben. Die Zuleitung von Randdaten an die Strafverfolgungsbehörden beschlage nur die strafprozessuale und nicht die verwaltungsrechtliche Seite der Überwachung des Fernmeldeverkehrs. Dafür seien die Staatsanwaltschaft und die Genehmigungsbehörde nach StPO zuständig. Der Dienst ÜPF sei dafür nicht zuständig.
5. 15. Dezember 2016, Einreichen der Beschwerde in öffentlich-rechtlichen Angelegenheiten an das Bundesgericht mit im Wesentlichen denselben Anträgen wie im Gesuch an den Dienst ÜPF und der Beschwerde an das Bundesverwaltungsgericht.
6. 2. März 2018, Urteil des Bundesgerichts: Es weist die Beschwerde ab, soweit es darauf eintritt. Es tritt dabei nicht auf den Antrag ein, dass der Anbieterin zu verbieten sei, Daten an die Behörden herauszugeben.

F. Statement of alleged violation(s) of the Convention and/or Protocols and relevant arguments

59. Article invoked	Explanation
Art. 8 EMRK, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108 des Europarates) Art. 17 UNO-Pakt II, Art. 13 EMRK	Durch die Vorratsdatenspeicherung sehr viele Metadaten gespeichert. Aus diesen Daten, u.U. in Kombination mit anderen Daten, sind sehr genaue Schlüsse auf das Privatleben der Betroffenen möglich, u.a. auf Standorte, Kommunikationspartner, Gewohnheiten, Tätigkeiten und soziale Beziehungen. Solche Informationen sind genauso sensibel wie der Inhalt der Kommunikationen selbst. Die Speicherung der Daten kann bei diesen das Gefühl erzeugen, dass ihr Privatleben Gegenstand ständiger Überwachung ist mit der Folge, dass sie ihr Kommunikationsverhalten anpassen und einschränken («chilling effect»). Die Verwendung der Daten in einem Strafverfahren kann zu einem Verdacht auf eine strafbare Handlung führen, gegen sich die betroffene Person wehren muss. Die Vorratsdatenspeicherung greift bereits durch die Speicherung an sich sehr stark ins Recht auf Achtung des Privat- und Familienlebens ein, welches das Recht garantiert, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Die gesetzliche Grundlage ist unzureichend. Die Details der Datenspeicherung und ihrer Verwendung ergeben sich nicht aus dem Gesetz selbst, sondern nur aus untergeordneten, demokratisch nicht genügend legitimierten Verordnungen und Richtlinien, die so abstrakt und technisch komplex sind, dass die Rechtsunterworfenen die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe nicht ermessen können. Die Vorratsdatenspeicherung ist in dieser Form nicht notwendig, sie ist unverhältnismässig und mangels entsprechenden Belege durch den Staat kann nicht von deren Wirksamkeit ausgegangen werden. Sie erstreckt sich grundsätzlich auf alle Personen, alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten und hält alle Daten während mindestens sechs Monaten vor, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme vorzusehen, ohne dass die betroffenen Personen auch nur mittelbar oder entfernt Anlass zur Strafverfolgung geben könnten und ohne dass ein direkter, objektiver Zusammenhang zwischen den auf Vorrat gespeicherten Daten und der Bedrohung für die öffentliche Sicherheit gegeben sein müsste. Die Speicherung und Nutzung der Daten zielt auch auf relativ geringfügige Delikte und beschränkt sich nicht auf die Bekämpfung von schwerer Kriminalität. Sie geht damit weit über das für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer Notwendige hinaus. Der Datenschutz und der Schutz vor Datenmissbrauch sind ungenügend. Der Beschwerdeführer ist konkret wie im Sachverhalt beschrieben von der Vorratsdatenspeicherung betroffen. Er ist dadurch in schwer wiegender Weise von der Vorratsdatenspeicherung betroffen und in seinen Ansprüchen aus Art. 8 EMRK verletzt.
Art. 10 EMRK, Art. 13 EMRK	Die Vorratsdatenspeicherung verletzt den Beschwerdeführer auch in der Freiheit der Meinungsäusserung, da die vom Beschwerdeführer für den Meinungsaustausch genutzten üblichen elektronische Kommunikationskanäle durch die Vorratsdatenspeicherung überwacht werden. Dies erzeugt beim Beschwerdeführer das Gefühl, permanent überwacht zu sein, und führt dazu, dass er sein Kommunikationsverhalten dieser Überwachungssituation anpasst und seine Kommunikation einschränkt, sich also insoweit selbst in der Ausübung seiner Freiheiten einschränkt, insbesondere in seiner Tätigkeit als Journalist («chilling effect»). Aus denselben Gründen wie im Zusammenhang mit Art. 8 EMRK dargelegt erscheint auch der Eingriff in Art. 10 EMRK nicht als gerechtfertigt und geht weit über das hinaus, was in einer demokratischen Gesellschaft für die gemäss Art. 10 EMRK zulässigen Zwecke notwendig ist. Der Beschwerdeführer ist als Journalisten darauf angewiesen, frei von Überwachung und unter Wahrung des Quellenschutzes recherchieren und andere Personen kontaktieren zu können. Der Schutz journalistischer Quellen ist eine der Grundbedingungen der Medienfreiheit. Geschützt ist namentlich die Identität des Autors sowie Inhalt und Quelle der Information. Medienschaffende können ihre Aufgabe als Informationsvermittler und Wächter nur erfüllen, wenn sie die erforderliche Information von Dritten erhalten, insbesondere Hinweise auf Vorkommnisse von gesellschaftlichem Interesse, die sonst verborgen bleiben würden.

Statement of alleged violation(s) of the Convention and/or Protocols and relevant arguments (continued)

60. Article invoked	Explanation
	Dies setzt voraus, dass die Informationsgeber darauf vertrauen können, dass ihr Name nicht preisgegeben wird, andernfalls könnten diese von der Preisgabe der anvertrauten Informationen abgeschreckt sein («chilling effect»). Nur zwingende Gründe des öffentlichen Interesses vermögen die Aufhebung des Redaktionsgeheimnisses zu rechtfertigen. Die Vorratsdaten verletzen den Quellenschutz, weil, wie im Sacherhalt dargelegt, aus Vorratsdaten Schlüsse auf Quellen des Beschwerdeführers gezogen werden können, ohne dass zwingende Gründe dafür bestehen. Es fehlen, wie im Sachverhalt dargelegt, zuverlässig funktionierenden Mechanismen, welche zu verhindern vermöchten, dass Vorratsdaten, welche den Quellenschutz tangieren, in einem Strafprozess verwendet werden und so den Quellenschutz durchbrechen. Gemäss Art. 271 Abs. 3 StPO sind Informationen von Personen, welche das Zeugnis verweigern können (dazu gehören auch Journalisten), aus den Akten auszusondern und sofort zu vernichten. Dies gewährleistet den Quellenschutz nicht. Die dem Quellenschutz unterliegenden Daten werden dennoch gespeichert. Regelmässig werden die Strafverfolgungsbehörden zumindest beim Erhalt der Daten nicht feststellen können, wenn Daten dem Quellenschutz unterliegen. Die Feststellung eines Gerichts oder einer Behörde, dass die Daten dem Quellenschutz unterliegen, setzt Kenntnis über die Kommunikationsteilnehmer und dem Umstand voraus, dass hier ein Journalist und seine Quelle kommunizieren. Gerade damit wird der Quellenschutz durchbrochen. Der Journalist und/oder seine Quelle werden in vielen Fällen gar nicht davon erfahren, dass sie betreffende Vorratsdaten von den Strafverfolgungsbehörden verwendet werden, und können sich dann auch nicht dagegen wehren. Je nach Konstellation haben sie keine prozessualen Rechte, um sich gegen die Verwendung der Daten zu wehren. Um die Aussonderung der betreffenden Daten zu erreichen müssten sie paradoxerweise genau das geltend machen, was den Behörden zur Gewährleistung des Quellenschutzes nicht zur Kenntnis gelangen sollte, nämlich die Tatsache, dass ein Journalist und seine Quelle miteinander kommunizieren. Ein effektiver Schutzmechanismus, welcher sicherstellt, dass die Behörden keine dem Quellenschutz unterliegende Informationen erhalten oder nur in Fällen, in denen dies als durch zwingende Gründe gerechtfertigt ist, besteht damit nicht. Bereits die Speicherung von Vorratsdaten, welche sich auf die Kommunikation des Beschwerdeführers mit Quellen beziehen, verletzt den Anspruch auf Quellenschutz, die Medienfreiheit und die Meinungsäusserungsfreiheit. Potenzielle Informationsgeber des Beschwerdeführers können nicht darauf vertrauen, dass ihre Quelleneigenschaft den Behörden trotz der Speicherung der betreffenden Daten nicht bekannt wird, was sie davon abschrecken kann, sich als Quelle zur Verfügung zu stellen. Dies beeinträchtigt die journalistische Aufgabe des Beschwerdeführers als Informationsvermittler und Wächter. Der Beschwerdeführer ist wie im Sachverhalt und wie in der Begründung zu Art. 8 EMRK dargelegt stark von der Vorratsdatenspeicherung betroffen. Die Vorratsdatenspeicherung verletzt ihn in seinen Ansprüchen aus Art. 10 EMRK.
Art. 11 EMRK, Art. 13 EMRK	Die Vorratsdatenspeicherung verletzt auch die Freiheit des Beschwerdeführers, sich friedlich mit anderen zu versammeln, da die vom Beschwerdeführer die Vorratsdatenspeicherung dafür genutzt werden kann, zu eruieren, wer an einer Versammlung teilgenommen hat und mit wem mutmassliche Versammlungsteilnehmer kommuniziert haben. Dies schränkt den Beschwerdeführer in der Nutzung der Kommunikationskanäle wie unter Art. 10 EMRK beschrieben ein. Aus denselben Gründen wie im Zusammenhang mit Art. 8 EMRK dargelegt erscheint auch der Eingriff in Art. 11 EMRK nicht als gerechtfertigt und geht weit über das hinaus, was in einer demokratischen Gesellschaft für die gemäss Art. 11 EMRK zulässigen Zwecke notwendig ist. Der Beschwerdeführer ist wie im Sachverhalt und wie in der Begründung zu Art. 8 EMRK dargelegt stark von der Vorratsdatenspeicherung betroffen. Die Vorratsdatenspeicherung verletzt ihn in seinen Ansprüchen aus Art. 11 EMRK.
Art. 6 EMRK	Schliesslich ist Unschuldsvermutung verletzt (Art. 6 EMRK), weil der Beschwerdeführer gewärtigen muss, dass Daten, welche er durch seine gewöhnliche Kommunikation auf elektronischem Weg erzeugt, als Beweismittel gegen ihn verwendet werden.

- Please ensure that the information you include here does not exceed the pages allotted -

G. Compliance with admisibility criteria laid down in Article 35 § 1 of the Convention

For each complaint, please confirm that you have used the available effective remedies in the country concerned, including appeals, and also indicate the date when the final decision at domestic level was delivered and received, to show that you have complied with the six-month time-limit.

61. Complaint	Information about remedies used and the date of the final decision
Art. 8 EMRK, Art. 13 EMRK	Verfügung des Dienstes ÜPF vom 30. Juni 2014 über das Gesuch an den Dienst ÜPF vom 20. Februar 2014 Urteil des Bundesverwaltungsgerichts vom 9. November 2016, A-4941/2014, über die Beschwerde an das Bundesverwaltungsgericht vom 2. September 2014 Urteil des Bundesgerichts, 2. März 2018, 1C_598/2016, über die Beschwerde an das Bundesgericht vom 15. Dezember 2016
Art. 10 EMRK, Art. 13 EMRK	Verfügung des Dienstes ÜPF vom 30. Juni 2014 über das Gesuch an den Dienst ÜPF vom 20. Februar 2014 Urteil des Bundesverwaltungsgerichts vom 9. November 2016, A-4941/2014, über die Beschwerde an das Bundesverwaltungsgericht vom 2. September 2014 Urteil des Bundesgerichts, 2. März 2018, 1C_598/2016, über die Beschwerde an das Bundesgericht vom 15. Dezember 2016
Art. 11 EMRK, Art. 13 EMRK	Verfügung des Dienstes ÜPF vom 30. Juni 2014 über das Gesuch an den Dienst ÜPF vom 20. Februar 2014 Urteil des Bundesverwaltungsgerichts vom 9. November 2016, A-4941/2014, über die Beschwerde an das Bundesverwaltungsgericht vom 2. September 2014 Urteil des Bundesgerichts, 2. März 2018, 1C_598/2016, über die Beschwerde an das Bundesgericht vom 15. Dezember 2016
Art. 6 EMRK	Verfügung des Dienstes ÜPF vom 30. Juni 2014 über das Gesuch an den Dienst ÜPF vom 20. Februar 2014 Urteil des Bundesverwaltungsgerichts vom 9. November 2016, A-4941/2014, über die Beschwerde an das Bundesverwaltungsgericht vom 2. September 2014 Urteil des Bundesgerichts, 2. März 2018, 1C_598/2016, über die Beschwerde an das Bundesgericht vom 15. Dezember 2016

- Please ensure that the information you include here does not exceed the page allotted -

62. Is or was there an appeal or remedy available to you which you have not used?
- ○ Yes
- ◉ No

63. If you answered Yes above, please state which appeal or remedy you have not used and explain why not

H. Information concerning other international proceedings (if any)

64. Have you raised any of these complaints in another procedure of international investigation or settlement?
- ○ Yes
- ◉ No

65. If you answered Yes above, please give a concise summary of the procedure (complaints submitted, name of the international body and date and nature of any decisions given).

66. Do you (the applicant) currently have, or have you previously had, any other applications before the Court?
- ○ Yes
- ◉ No

67. If you answered Yes above, please write the relevant application number(s) in the box below.

I. List of accompanying documents

You should enclose full and legible copies of all documents. No documents will be returned to you. It is thus in your interests to submit copies, not originals. You MUST:

- **arrange the documents in order by date and by procedure;**
- **number the pages consecutively; and**
- **NOT staple, bind or tape the documents.**

68. In the box below, please list the documents in chronological order with a concise description. Indicate the page number at which each document may be found.

Any other comments

Do you have any other comments about your application?

69. Comments

Declaration and signature

I hereby declare that, to the best of my knowledge and belief, the information I have given in the present application form is correct.

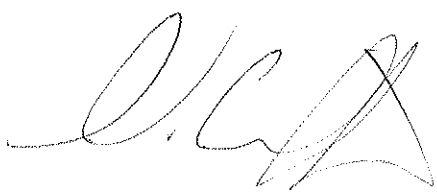
70. Date

2	7	0	9	2	0	1	8
D	D	M	M	Y	Y	Y	Y

e.g. 27/09/2015

The applicant(s) or the applicant's representative(s) must sign in the box below.

71. Signature(s) ○ Applicant(s) ● Representative(s) - tick as appropriate



Confirmation of correspondent

If there is more than one applicant or more than one representative, please give the name and address of the one person with whom the Court will correspond. Where the applicant is represented, the Court will correspond only with the representative (lawyer or non-lawyer).

72. Name and address of ○ Applicant ○ Representative - tick as appropriate

The completed application form should be signed and sent by post to:

The Registrar
European Court of Human Rights
Council of Europe
67075 STRASBOURG CEDEX
FRANCE

893669e1-66ca-4653-b9c0-2de2561a694b

Ergänzung zu Ziff. E. der Beschwerde (Sachverhalt):

1. (ad 3.) Indem das Gesetz grundsätzlich jedes Vergehen als Straftat erachtet, für deren Verfolgung Vorratsdaten genutzt werden dürfen, gibt es eine abstrakte Wertung vor, gemäss der die Nutzung nicht auf die Verfolgung schwerer Straftaten beschränkt ist, was in der Praxis auch so gehandhabt wird, so das effektiv relativ geringfügige Delikte für die Nutzung von Vorratsdaten ausreichen. Als Vergehen ausgestaltete Delikte sind etwa falscher Alarm (Art. 128bis StGB), Sachbeschädigung (Art. 144 StGB), Zechprellerei (Art. 149 StGB), Beschimpfung (Art. 177 StGB), Beschäftigung von Ausländerinnen und Ausländern ohne Bewilligung (Art. 117 AuG), Missachtung der Ein- oder Ausgrenzung (Art. 119 AuG) und Fahren ohne Berechtigung (Art. 95 SVG).
2. (ad 6.) Erfasst werden offenbar insbesondere folgende Daten:
2.1. Grunddaten des betreffenden Kunden: Name, Adresse, Geburtsdatum, Ausweis/Ausweisnummer, Beruf, Telefonnummer(n), Mail-Adresse(n), Bei Firmen: Firma, Firmennummer (Zefix), Kontaktperson, Kunde seit bzw. von/bis
2.2. Telefon: Telefonnummer, Telefonnummer der Gegenseite, Telefon-Anbieter, Telefon-Abo, Dauer des Abos, Art des Anschlusses, Angaben zum Anschlussinhaber, einschliesslich Adresse(n)/ Mail-Adresse(n), Details zu Zahlungen für den Anschluss (Art der Zahlung, Inhaber, Bank, Kontonummern) Details zu Kosten/Zahlung des Gesprächs (in den Richtlinien wird darauf verwiesen, dass gewisse zusätzliche Informationen, die nicht Bestandteil der Vorratsdatenspeicherung sind, über die strafprozessuale Editionspflicht erhältlich gemacht werden können, insb. weitere Zahlungsinformationen und gewählte Extensions während des Telefongesprächs (DTMF)eiten, insb. Beginn und Ende Anruf, Art der Verbindung/Kommunikation, allfällige Umleitungen/Weiterleitungen bei der Kommunikation); zusätzlich bei Anrufen via Festnetz: Adresse des Anschlusses, verwendetes Gerät; zusätzlich bei Anrufen via Mobiltelefon: IMSI (auf SIM gespeicherte, eindeutige Nummer), IMEI (eindeutige Nummer des Telefongerätes), pUK- und pUK2-Code (PIN-Unlock-Keys [Codes zum Entsperren der SIM]), Zeiten, insb. Beginn und Ende der Verbindung zu den im Gespräch genutzten Antennen, benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung; zusätzlich bei SMS oder MMS: Angaben zu Art, Status, Übertragung der SMS bzw. MMS, Mail-Adresse bei Übertragung via Mail-Gateway
2.3. Mail: Mail-Adressen, inkl. Aliases, Mail-Konto-Inhaber, einschliesslich Adresse und Mail, Dauer des Mail-Kontos, Details zu Zahlungen für das Mail-Konto (Art der Zahlung, Inhaber, Bank, Kontonummern), Mail-Adresse Absender, Mail-Adresse Empfänger, Zeitangaben zur Übertragung des Mails, Übertragungsprotokoll, Übertragungsart des Mails (POP, IMAP, Webmail), Übertragungsstatus des Mails, IP-Adressen der kommunizierenden Stellen

(z.B. Absender und Mailserver), Message ID, Verbindungsaufnahmen zum Mail-Server

2.4. Internet: Provider, Internet-Abo, IP-Adresse, MAC-Adresse (eindeutige Nummer des Gerätes), Lokalisation, Art und weitere Eigenschaften des Modems bzw. Routers und der Einwahl, Angaben zum Kunden, einschliesslich Adresse(n)/Mail-Adresse(n), Details zu Zahlungen für das Internet-Abo (Art der Zahlung, Inhaber, Bank, Kontonummern), zusätzlich bei Internet-Verbindungen über Mobilfunk: benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung, benutzter Port

2.5. Multimedia (Voice over IP [VoIP]-Telefonie, Videotelefonie, etc.): Provider der Multimedia-Kommunikation, Telefonnummer, SIP-URI (sofern vorhanden), IMSI (sofern vorhanden), Multimedia-Service-Typ; Beginn, Ende und Dauer der Kommunikation, Rolle in der Kommunikation, Adresse, Details zu Zahlungen (Art der Zahlung, Inhaber, Bank, Kontonummern), IP-Adresse, ausgehender Port, Port auf der Gegenseite (auch bei Kommunikation über Mobilfunknetz)

2.5. Brief- und Paketpost: Angaben zu Absender und Empfänger von Postsendungen (soweit vorhanden)

3. (ad 8.)

3.1. Die Praxis lässt verschiedene ausgeweitete Nutzungen der Vorratsdaten zu, aus welchen deutlich wird, dass für die betroffenen Personen kaum zu ermessen ist, welche Tragweite die Vorratsdatenspeicherung hat.

3.2. Darunter fällt die Rasterfahndung in gespeicherten Antennenstandorten (sog. Antennensuchlauf, vgl. 1B_376/2011 sowie Simon Schlauri, Fernmeldeüberwachung à discrétion?, in: sic! 2012, S. 238, S. 240 f.). Die Rechtsunterworfenen werden sich kaum bewusst sein, dass jedes Mal, wenn sie ihr Mobiltelefon verwendet (bzw. das Mobiltelefon für gewisse, vom Benutzer u.U. nicht einmal wahrgenommene Funktionen aktiviert wird), der Antennenstandort samt Hauptstrahlrichtung gespeichert wird, und dass ihr effektiver Standort damit sehr genau, u.U. auf wenige Meter genau, erfasst wird, und dass diese Daten dafür verwendet werden können, sie in eine Rasterfahndung einzubeziehen, wenn die Strafverfolgungsbehörde im Rahmen einer entsprechenden Strafuntersuchung wissen möchte, wer sich in den letzten sechs Monaten in einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hat. Der Antennensuchlauf ist zudem nur in der Verordnung vorgesehen (Art. 16 lit. e VÜPF) und verfügt damit nicht über eine genügende gesetzliche Grundlage, zumal sie einen schweren Eingriff in die Grundrechte darstellt. Hinzu kommt, dass die meisten Personen, deren Daten in eine solche Rasterfahndung einbezogen werden, hernach nicht über die Verwendung ihrer Daten benachrichtigt werden.

3.3. Mit der Kopfschaltung wird eine weitere Überwachungsart praktiziert, welche zu einer Massenüberwachung führt. Bei dieser Überwachungsart werden sämtliche Gespräche überwacht, die von einem beliebigen Anschluss

in der Schweiz auf einen bestimmten Anschluss im Ausland oder von diesem Anschluss im Ausland auf einen beliebigen Anschluss in der Schweiz getätigt werden. Damit werden im Ergebnis sämtliche Schweizer Anschlüsse auf ihre allfälligen Verbindungen zu einem bestimmten ausländischen Anschluss überwacht. Den Strafverfolgungsbehörden werden in erster Linie eruieren wollen, ob und mit welchen Gegenstellen innerhalb der Schweiz sich ein bestimmter ausländischer Anschluss verbindet. Technisch wird dies allerdings dadurch erreicht, dass die Verbindungsdaten sämtlicher Schweizer Anschlüsse entsprechend gescannt und somit überwacht werden.

3.4. Die Vorratsdatenspeicherung verpflichtet die Internetzugangs–Anbieterinnen, die von ihr dynamisch einem Kundenanschluss zugewiesene IP-Adresse für 6 Monate zu speichern. Damit lassen sich rückwirkend aus den in den Logfiles der aufgerufenen Server und Dienste gespeicherten Source-IP-Adressen den Kunden identifizieren (wobei diese Speicherung der IP-Adressen in den Serverlogfiles datenschutzrechtlich zeitlich nur sehr eingeschränkt erlaubt wäre, da es sich hierbei offensichtlich um personenbezogene resp. nach Datenschutzgesetz auf Personen beziehbare Daten handelt). Falls nun ein NAT-Verfahren genutzt wird, was in praktisch allen Mobilfunknetzen und (öffentlichen) WLANs der Fall ist, muss vom Provider zusätzlich die Informationen aus der NAT-Tabelle des Routers für 6 Monate gespeichert werden. Aus diesen Tabellen ist ersichtlich, welches Gerät (Client) mit welcher IP mit welchem Router verbunden gewesen ist und über welche Ports die Kommunikation dabei lief. Die Speicherung dient dazu, Antwortdatenpakete einzelnen Clients zuordnen zu können. Der Begriff «Netzwerkadressübersetzung» (Network Address Translation, NAT) fasst verschiedene Verfahren zusammen, welche in Datenpaketen automatisiert Adressinformationen durch andere ersetzen. Die Netzwerkadressübersetzung kommt in der Regel auf Routern zum Einsatz, die verschiedene Netzwerke miteinander verbinden. Das Verfahren «Source-NAT» wird meist verwendet, wenn zuwenig öffentliche IPv4-Adressen zur Verfügung stehen, die den Geräten (Clients) zugewiesen werden können, die mit dem Internet kommunizieren möchten. NAT ermöglicht in diesen Fällen die Verwendung mehrerer privater IP-Adressen mit nur einer öffentlichen IP-Adresse. Dabei wird bei jedem Verbindungsaufbau durch einen internen Client die interne Quell-IP-Adresse durch die öffentliche IP-Adresse des Routers ersetzt. Zudem wird der Quellport des internen Clients durch einen freien Port des Routers ersetzt, der dadurch belegt wird. Diese Zuordnung wird in der NAT-Table des Routers gespeichert. Damit lassen sich Antwortdatenpakete vom NAT-Router auch wiederum an den korrekten Client zurück senden. (vgl. https://de.wikipedia.org/wiki/Netzwerkadressübersetzung). Daher lässt sich über die gespeicherten Daten aus NAT-Tabellen eruieren, an welchen Client Antwortdatenpakete gegangen sind. Daraus wiederum kann geschlossen werden, welche Server und Dienste (etwa Websites) dieser Client aufgerufen

hat. Soweit die gespeicherten Daten aus NAT-Tabellen einem konkreten Client zugeordnet werden können, erlaubt dies im Prinzip auch die Erstellung von detaillierten Bewegungsprofilen. Ungeachtet dessen erteilt kein Provider Auskunft über die entsprechenden Daten aus NAT-Tabellen von Routern, die bei ihm gespeichert sind, wenn ein Kunde von seiner Möglichkeit, vom Provider Auskunft über die ihn betreffenden Daten der Vorratsdatenspeicherung zu erhalten, Gebrauch macht.

4. (ad 9.)

4.1. Die Vorratsdatenspeicherung verletzt eine Reihe von datenschutzrechtlichen Grundsätzen, namentlich das Verbot des Datensammelns auf Vorrat, den Grundsatz der Zweckbindung der Daten und den Grundsatz der Verhältnismässigkeit der Datenbearbeitung (vgl. dazu Art. 4 ff. DSG; Urs Maurer-Lambrou/Andrea Steiner, Balser Kommentar DSG, 2. Aufl., Basel 2006, Art. 4 N 9 ff.; Astrid Epiney, in: Belser/Epiney/Waldmann, Datenschutzrecht, Bern 2011, § 9 N 23 ff.). Die Daten dienen eigentlich dazu, dass die gewünschte Kommunikation technisch stattfinden kann. Die systematische Speicherung dieser Daten für die allfällige Verwendung in einem späteren Strafverfahren ihren Zweck grundlegend. Es wäre erforderlich, dass die betroffene Person der Sammlung der Daten freiwillig zustimmt, nachdem sie angemessen informiert worden ist. Dies ist bei der Vorratsdatenspeicherung nicht der Fall. Die Verletzung datenschutzrechtliche Grundsätze durch einen Anbieter hat in aller Regel keine verwaltungsrechtlichen oder strafrechtlichen Folgen.

4.2. Es ist nicht sichergestellt, dass die Daten nicht ins Ausland gelangen, etwa im Rahmen internationaler Rechtshilfe in Strafsachen, polizeilicher und geheimdienstlicher Zusammenarbeit, aber auch, weil ein Provider seine Daten im Ausland lagern lässt oder aufgrund von mangelnder Datensicherheit. Offensichtlich verwalten betroffene Provider tatsächlich sensible Daten im Ausland. Wenn die Daten ins Ausland gelangen ist die Einhaltung der in der Schweiz geltenden Garantien bezüglich Grundrechte, Datenschutz und Datensicherheit nicht gewährleistet. Diese Problematik kann nicht unter Verweis auf abstrakte Regelungen zum Datenschutz und zur Datensicherheit beseite gewischt werden, zumal die im Ausland gelegenen Daten auch dem dortigen Recht unterstehen und dies den zu gewährleistenden Schutz vor Missbrauch unterlaufen kann, womit es griffiger internationaler Regelungen bedürfte.

4.3. Die grosse Menge an Daten, die bei diversen Anbietern anfallen, werfen beträchtliche Probleme bezüglich der Datensicherheit auf. Die Daten werden nicht vom Dienst ÜPF oder von den Strafverfolgungsbehörden gesammelt, sondern müssen von den Anbietern gespeichert werden. Dies schützt zwar die Daten vor dem unmittelbaren staatlichen Zugriff. Die Daten müssen aber von den Anbietern vor unbefugten Zugriffen geschützt werden. Art. 9 VÜPF überträgt den Anbietern, für die Datensicherheit besorgt zu sein, und verweist zudem auf die VDSG, welche für die Anbieter ohnehin gelten

würde, und die BinfV, welche inhaltlich nichts Wesentliches zum Problem beiträgt. Dies genügt nicht. Damit stellt der Staat nicht sicher, dass die Daten sicher gehandhabt werden. Es fehlen griffige Vorschriften zur Datensicherheit, und es fehlt an einer Durchsetzung und Kontrolle der Datensicherheit von staatlicher Seite. Der Dienst ÜPF selbst wird im Übrigen auch nicht zureichend kontrolliert. Zwar besteht u.a. eine parlamentarische Kontrolle der Tätigkeit des Dienstes ÜPF, diese kann aber nur von Zeit zu Zeit einzelne Aspekte der Tätigkeit des Dienstes ÜPF kontrollieren und erstreckt sich offenbar nicht auf die im ISC-EJPD angesiedelte Informatik, auf der die Praxis der Vorratsdatenspeicherung Seitens des Dienstes ÜPF beruht.

4.4. Effektiv ist die Datensicherheit offensichtlich nicht gewährleistet. Konkrete Vorfälle, die bekannt geworden sind, zeigen, dass dies kein hypothetisches Problem darstellt, sondern ein reales.

4.5. Auf welcher Software und Hardware die Speicherung und Nutzung der Vorratsdaten seitens der Anbieter und seitens des Dienstes ÜPF beruht, ist nicht bekannt. Es kann ohne genauere Kenntnis diesbezüglich nicht angenommen werden, dass die gespeicherten Daten damit hinreichend geschützt sind. Angesichts der grossen Menge und der hohen Sensibilität der Daten müsste der Schutz der Daten auf technischer Seite sehr hohen Ansprüchen genügen. Das Risiko, dass ausländische staatliche Stellen oder nichtstaatliche Hacker versuchen, an diese Daten heranzukommen, ist nicht zu unterschätzen. Es sei hier auf die bekannten ungeheuren Aktivitäten der amerikanischen National Security Agency (NSA) und mit ihr verbundener Dienste verwiesen. Es ist überdies stets damit zu rechnen, dass ein Anbieter von Soft- und Hardware für Belange der Vorratsdatenspeicherung mit der NSA oder anderen Diensten verknüpft ist, indem er auch der NSA oder anderen Diensten Soft- und Hardware liefert oder indem er sonstwie auf freiwilliger oder unfreiwilliger Basis mit den entsprechenden Diensten zusammenarbeitet, u.a., indem er ihm Kenntnisse über Sicherheitslücken weitergibt.

4.6. Die mangelhafte Datensicherheit kann auch dazu führen, dass die Daten mit irgendwelchen anderen Absichten zweckentfremdet werden, z.B., um betroffene Personen zu kompromittieren oder zu erpressen. Beispiele aus dem amerikanischen Geheimdienst zeigen, dass dies nicht nur ein theoretisches, sondern ein reales Risiko ist.

4.7. Zu beachten ist auch die effektive Informatikpraxis, in der – auf Grund der geringeren, technischen Regelkomplexität – Datensicherungen (Backups) oftmals unterschiedslos von allen Daten auch für längere Zeit angelegt werden (zumal um Systeme im Störungsfall vollständig wiederherstellen zu können und dies auch für längere Zeit als bloss sechs Monate zurück).

5. (ad 12.)

5.1. Das inzwischen in Kraft getretene nBÜPF und das Nachrichtendienstgesetz (NDG) erlauben auch dem Nachrichtendienst die Nutzung der Vorratsdaten. Das NDG ermöglicht sog.

genehmigungspflichtige Beschaffungsmassnahmen, darunter die Nutzung der Vorratsdaten (Art. 26 Abs. 1 lit. a NDG). Bei der Nutzung der Vorratsdaten durch den Nachrichtendienst sind die strafprozessualen Garantien nicht gegeben. Es bedarf für die Nutzung in diesem Rahmen auch keines konkreten Tatverdachts. Voraussetzung ist, dass eine konkrete Bedrohung im Sinne von Artikel 19 Absatz 2 Buchstaben a–d NDG gegeben ist (Terrorismus, verbotener Nachrichtendienst, Proliferation oder Angriff auf eine kritische Infrastruktur) oder die Wahrung weiterer wichtiger Landesinteressen nach Artikel 3 NDG dies erfordert. Diese Voraussetzungen sind äusserst schwammig. Insbesondere wird, wenn der Nachrichtendienst solches behauptet, vom Gericht, das die Massnahme genehmigen muss, schlechterdings nicht zu überprüfen sein, ob die insinuierte Bedrohung und die Relevanz der von der Überwachung betroffenen Person diesbezüglich gegeben sind oder nicht. Das Gericht wird nur überprüfen können, ob der Nachrichtendienst des Bundes (NDB) Behauptungen aufstellt, die den gesetzlichen Anforderungen entsprechen. Die betroffene Person erfährt davon nichts und wird auch im Nachhinein regelmässig nicht über die Massnahme unterrichtet werden. Jede von der Vorratsdatenspeicherung betroffene Person läuft somit Gefahr, Ziel einer solchen genehmigungspflichtigen Massnahme zu werden, ohne dass ein Tatverdacht für eine strafbare Handlung besteht, und allfällige Vermutungen des NDB, welche die Person zum Ziel der Massnahme machen, müssen keineswegs zutreffend sein, so dass die betroffene Person u.U. Ziel der Massnahme wird, ohne konkret Anlass dazu gegeben zu haben. Nachdem der NDB überdies nach Art. 61 NDG Personendaten oder Listen von Personendaten ins Ausland bekannt geben kann, ist die Einhaltung der Grundrechte bei Vorratsdaten, die dem NDB geliefert werden, erst recht nicht gewährleistet.

6. (ad 13. ff.)

6.1. Zwar bezieht sich Art. 271 StPO auch auf den Quellenschutz von Journalisten. Ein effektiver Schutz der Grundrechte des Journalisten in Bezug auf die Verwendung von Daten aus der Vorratsdatenspeicherung resultiert daraus nicht. Vom Wortlaut her ist nicht einmal klar, ob sich Art. 271 StPO auf die Auskunft über Vorratsdaten nach Art. 273 StPO bezieht. Abgesehen schützt Art. 271 StPO den Journalisten bzw. seine Grundrechte nicht zureichend. Gerade bei Vorratsdaten lässt sich nicht vermeiden, dass diese der Strafverfolgungsbehörde zur Kenntnis gelangen, bevor die Mechanismen, wie sie in Art. 271 StPO vorgesehen sind, greifen können.

6.2. Die gesetzlich vorgesehene Beschränkung der Zulässigkeit von Direktschaltungen lässt sich in der Praxis seit einigen Jahren nicht mehr durchsetzen, da es kurz gesagt technisch gesehen im aktuellen System nur noch Direktschaltungen gibt. Die Ermittlungsbehörden von Bund und Kantonen können jederzeit und unmittelbar auf die aufgezeichneten Gespräche etc. zugreifen. Die Bestimmung von Art. 274 Abs. 4 lit. b StPO, wonach sich das Zwangsmassnahmengericht zur Zulässigkeit von

Direktschaltungen äussern muss, ist damit obsolet (Niklaus Schmid, Handbuch des Schweizerischen Strafprozesses, Zürich/St. Gallen 2009, N 1146; Hansjakob, StPO-Kommentar, Art. 271 StPO N 11; BaslerKomm/Jean-Richard-Dit-Bressel, Art. 269 StPO N 12, Art. 271 StPO N 10, Art. 274 StPO N 8).

6.3. Die Vorschrift, bei der Überwachung von Drittpersonen seien Informationen, die dem Zeugnisverweigerungsrecht unterliegen, aus den Akten zu nehmen, und die entsprechenden Informationen würden einem Verwertungsverbot unterliegen, genügt zum Schutz des Journalisten bzw. seiner Quelle nicht. Man hat versucht, den Quellenschutz zu gewährleisten, indem man den Journalisten denselben Vorschriften unterstellt hat wie andere Geheimnisträger. Dabei hat der Gesetzgeber übersehen, dass es hier entscheidende Unterschiede gibt. Anders als etwa bei Anwälten, Geistlichen und Ärzten geht es beim Quellenschutz nicht nur um das Gegenüber des Geheimnisträgers, sondern mindestens ebenso um den Geheimnisträger selbst. Während dem der Schutz des Anwaltsgeheimnisses dem Klienten dienen soll, bezieht sich der Quellenschutz primär auf den Journalisten.

6.4. Art. 271 StPO gewährt dem Journalisten keinen wirksamem Schutz seiner Grundrechte. Zum Einen liegt die entscheidende Information, nämlich dass, wo und über welchen Kanal ein Journalist mit einer anderen Person kommuniziert hat, in den eingeholten Vorratsdaten selbst. Soweit es sich beim Kommunikationspartner um eine geschützte Quelle handelt, liegt die entsprechende Information den Strafverfolgungsbehörden mit der Einholung der Auskunft über die Vorratsdaten unmittelbar vor. Die Strafverfolgungsbehörden erlangen damit ohne Weiteres über den Kontakt mit einer anderen Person Kenntnis. Ist diese andere Person eine Quelle des Journalisten, ist der Quellenschutz damit ausgehebelt. Zum Anderen ist der Journalist weniger umfassend geschützt als etwa der Anwalt. Beim Anwalt ist grundsätzlich die gesamte Kommunikation in seiner Berufssphäre durch das Anwaltsgeheimnis geschützt. Beim Journalisten hingegen bezieht sich der Schutz nur auf seine Quelle, nicht auf irgendwelche andere Kontakte, da er nur insoweit über ein Zeugnisverweigerungsrecht verfügt. Absurderweise würde damit die Durchsetzung der Aussonderung und Unverwertbarkeit nach Art. 271 Abs. 3 StPO beim Journalisten voraussetzen, dass der Behörde, welche die Aussonderung vornimmt und sich der Unverwertbarkeit bewusst sein soll, gerade davon Kenntnis hat, dass es sich um eine Quelle handelt. Anders kann sie das – eben nur selektiv auf Quellen bezogene – Zeugnisverweigerungsrecht im konkreten Fall gar nicht berücksichtigen. Wenn es nun aber der Strafverfolgungsbehörden von sich aus oder aufgrund von Angaben der Quelle oder des Journalisten klar wird, dass sich die Kommunikation auf eine geschützte Quelle des Journalisten bezieht, ist der Quellenschutz unwiederbringlich verletzt. Das Wissen, wer die Quelle des Journalisten ist, ist dadurch in die Köpfe der damit befassten Strafverfolgungsbehörden gelangt. Eine nachherige Entfernung der

entsprechenden Daten ändert daran nichts, ebenso wenig ein Verwertungsverbot. Anders als etwa beim Anwalt, wo es in der Regel zentral um den Inhalt der Kommunikation gehen wird – etwa zwischen Angeschuldigtem und Verteidiger –, ist es beim journalistischen Quellenschutz primär entscheidend, dass keine entsprechenden Metadaten bekannt werden, welche Rückschlüsse auf die Kommunikationspartner ermöglichen.

6.5. Hinzu kommt, dass eine selektive Löschung der dem Zeugnisverweigerungsrecht des Journalisten unterstehenden Daten mitunter gar nicht möglich ist. In der Praxis ist eine teilweise Entfernung von Daten nicht oder nur eingeschränkt möglich. Grundsätzlich ist die Datenintegrität zu wahren. Die Ermittlungsbehörden von Bund und Kantonen können jederzeit und unmittelbar auf die aufgezeichneten Gespräche etc. zugreifen. Ein weiteres Problem besteht insoweit, als die überwachte Person ein Interesse haben kann, dass auch Kommunikationsdaten mit Geheimnisträgern Eingang in die Untersuchung finden. Werden solche Daten sofort ausgesondert und vernichtet, dann können sie nicht mehr ins Verfahren eingeführt werden, auch wenn dies die betreffende Person später beantragt. Schliesslich kommt es immer wieder vor, dass Kommunikation teilweise geschützte Geheimnisse betrifft, aber auch Passagen beinhaltet, die verwertbar sind. Die teilweise Löschung einzelner Kommunikationsvorgänge ist allerdings vom System her nicht möglich und wäre auch bedenklich aufgrund der damit verbundenen Missbrauchsgefahr. Es bedarf jedenfalls einer Anordnung durch die Staatsanwaltschaft, was wiederum voraussetzt, dass die Staatsanwaltschaft die entsprechenden Daten zuvor zur Kenntnis genommen hat (vgl. Hansjakob, StPO-Kommentar, Art. 271 StPO N 15 ff.).

6.6. Weil Überwachungsmassnahmen geheim sind, weiss der betroffene Journalist zunächst nichts von diesen, sondern wird allenfalls im Nachhinein darüber orientiert, was allerdings in der Praxis auch nicht in jeder Konstellation garantiert ist, insbesondere dann nicht, wenn der Journalist lediglich Verbindungspartner der überwachten Person ist. Werden Vorratsdaten aus einer Anordnung verwendet, bei der der Journalist selbst nicht Subjekt Massnahme ist, aber ihn betreffende Vorratsdaten herausgegeben werden, wird er nicht orientiert. Er hat nach h. L. nicht einmal ein Beschwerderecht, was der Praxis des EGMR widerspricht, gemäss der Gesprächspartner von überwachten Personen Anspruch auf eine wirksame Beschwerde nach Art. 13 EMRK haben. Wird die Aussonderung durch das Gericht vorgenommen, bevor die Betroffenen über die Massnahme orientiert sind, so ist der Journalist bei der Aussonderung nicht involviert, dies unabängig davon, ob ihn diese als überwachte Person oder sonstwie betrifft. In dieser Situation obliegt die Gewährleistung des Quellenschutzes den übrigen Beteiligten, also der mit der Auswertung betrauten Behörde und dem mit der Leitung betrauten Gericht. Dabei kann es sich wegen der Relativität des den Journalisten betreffenden

Zeugnisverweigerungsrechts ergeben, dass die anordnende Behörde von Tatsachen Kenntnis erhält, deren Schutz nach Art. 264 Abs. 1 StPO gerade bezweckt ist. Es ist für die involvierten Stellen auch nicht unbedingt ersichtlich, dass der Quellenschutz tangiert ist. Schliesslich besteht ein eigentlich unlösbares Problem, indem die involvierten Stellen einerseits zur Wahrung des Quellenschutzes realisieren müsste, dass dieser tangiert sein könnte. Hierfür müssten sie aber gewisse Kenntnis über die Daten haben, was beim Quellenschutz gerade zu dessen Verletzung führen kann (BaslerKomm, Jean-Richard-Dit-Bressel, Art. 271 StPO N 10 f.; 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.; Györffy, a.a.O., Rz. 24 ff.).

6.7. Es bestehen damit keine wirksamen Schutzmechanismen gegen die mit der Vorratsdatenspeicherung verbundene Kompromittierung des Quellenschutzes. Der Journalist muss damit rechnen, dass Vorratsdaten, die durch die Kommunikation mit Quellen anfallen, in einem Strafverfahren beigezogen werden und so seine Quellen offen legen. Der Quellenschutz ist damit durch die Vorratsdatenspeicherung beeinträchtigt und kann nicht mehr garantiert werden, sobald der Journalist Kommunikationsmittel verwendet, die der Vorratsdatenspeicherung unterliegen. Die mit der Vorratsdatenspeicherung verbundenen Einschränkungen der Grundrechte wiegen damit für ihn besonders schwer, einschliesslich des darin enthaltenen «chilling effects». Die Vorratsdatenspeicherung beeinträchtigt damit seine Arbeit bzw. seine Arbeitsweise nachhaltig, zumal er und seine potenziellen Quellen eigentlich essenziell auf Kommunikation und die Nutzung zeitgemässer Kommunikationskanäle angewiesen sind.

Ergänzung zu Ziff. F. der Beschwerde (Konventionsverletzungen, Beschwerdebegründung:

7. (ad EMRK 8, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates] Art. 17 UNO-Pakt II, Art. 13 EMRK)

7.1. Die Vorratsdatenspeicherung greift ins Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten, auf informationelle Selbstbestimmung auf persönliche Freiheit und Bewegungsfreiheit ein (Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Dies betrifft jede Form von Kommunikation, unabhängig davon, wo und mit welchen Mitteln die Kommunikation geführt wird. Geschützt ist sowohl der

Inhalt der Kommunikation als auch die Tatsache an sich, dass die Kommunikation stattfindet, namentlich Ort und Zeit der Kommunikation sowie die Identität der daran teilnehmenden Personen. Diese Grundrechte sind damit immer dann tangiert, wenn der Staat Daten im Zusammenhang mit der Kommunikation von Personen erfasst und speichert, und zwar sowohl, wenn der Inhalt der Daten gespeichert wird, als auch bei der Speicherung sogenannter Metadaten. Der schwere Eingriff liegt bereits in der Speicherung der Daten und der damit verbundenen Überwachung an sich (vgl. Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 203 ff.,).

7.2. Durch die heutige Verbreitung von elektronischen Kommunikationskanälen (insb. Smartphones, Tablets und Computer) fallen sehr viele Metadaten an. Insbesondere Mobiltelefone führen praktisch zu ständiger «Kommunikation» mit entsprechenden Metadaten (z.B. bei Push-Meldungen, der Nutzung von Streaming-Diensten wie Spotify oder Netflix oder Hintergrundaktivität von Apps). Die erlaubt u.a. extrem detaillierte Bewegungsprofile. Hinzu kommt, dass die im Rahmen der Vorratsdatenspeicherung erfassten Daten mit weiteren Daten kombiniert werden können, etwa bei der Nutzung von Daten im Zusammenhang mit IP-Adressen Tabellen von NAT-Routern, woraus je nachdem eruiert werden kann, wer wann welche Website mit welchem Inhalt geladen hat. Mit den auf Vorrat zu speichernden Daten können Quelle und Adressat der Kommunikation rückverfolgt und identifiziert werden, Datum, Uhrzeit, Dauer und Art der Kommunikation, die dabei verwendeten Geräte und deren Standort können bestimmt werden. Erfasst werden zudem weitere Daten wie Daten zur Person, insb. Adressen, Bankdaten, und Daten mit Bezug auf den Provider. Zu den erfassten Daten (auf Vorrat gesammelte Metadaten und Bestandesdaten) gehören Name und Anschrift des Teilnehmers oder registrierten Benutzers, die Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse und die MAC-Adresse und weitere Eigenschaften verwendeter Geräte. Aus diesen Daten geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand.

7.3. Die Schwere des Eingriffs ergibt sich auch aus der möglichen Nutzung der gespeicherten Daten im Strafverfahren. Die Strafverfolgungsbehörden können die gespeicherten Daten so interpretieren, dass sich daraus ein Verdacht auf eine strafbare Handlung ergibt, gegen sich die betroffene Person wehren muss, dies u.U. mit Mitteln wie dem Antennensuchlauf, der Kopfschaltung und der Interpretation von Daten aus NAT-Tabellen von Routern. Die betroffene Person hat dazu allenfalls gar keinen konkreten Anlass gegeben.

7.4. Die Vorratsdatenspeicherung beschränkt sich nicht auf eine gezielte Vorratsdatenspeicherung zu Bekämpfung schwerer Straftaten, sondern

erstreckt sich auf alle Personen, alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme vorzusehen. Sie betrifft unterschiedslos alle Personen, die elektronische Kommunikationsmittel benutzten, ohne dass diese auch nur mittelbar oder entfernt Anlass zur Strafverfolgung geben könnten. Ein direkter, objektiver Zusammenhang zwischen den auf Vorrat gespeicherten Daten und der Bedrohung für die öffentliche Sicherheit muss nicht bestehen. Sie beschränkt sich nicht auf Daten eines bestimmten Zeitraums, Gebiets oder eines Kreises von Personen, die in irgendeiner Weise in schwere Straftaten verwickelt sein oder aus anderen Gründen zur Verhütung oder Verfolgung solcher Delikte beitragen könnten. Die Daten werden für eine Mindestdauer von sechs Monaten gespeichert, ohne dass eine Unterscheidung der Datenkategorien je nach deren etwaigen Nutzen für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird.

7.5. Hinzu kommen die den Behörden eingeräumten Möglichkeiten der Nutzung der Daten. Diese Möglichkeiten sind bei der Gewichtung des mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffs zwingend zu berücksichtigen, auch wenn die auf Vorrat gespeicherten Daten nicht in jedem Fall genutzt werden. Der mit der Vorratsdatenspeicherung verbundene virtuelle Eingriff in die konventionsrechtlichen Garantien liegt nicht nur in deren Speicherung, sondern auch in allfälligen späteren Nutzung der gespeicherten Daten durch die Behörden. Zur Prüfung der Grundrechtskonformität der Vorratsdatenspeicherung gehört deshalb auch die Untersuchung der Frage, auf welche Art und Weise und unter welchen Voraussetzungen die Behörden die Daten später nutzen können. Verschiedene Aspekte, welche gemäss der Rechtsprechung der Strassburger Organe zur Beurteilung der Grundrechtskonformität zu berücksichtigen sind, lassen sich nicht ohne Einbezug der allfälligen Nutzung der Daten durch die Behörden beurteilen. Dies gilt namentlich für die Beurteilung, ob die Vorratsdatenspeicherung über die erforderliche gesetzliche Grundlage verfügt, ob sie als notwendig i.S.d. betroffenen Konventionsbestimmungen erscheint, ob Schutz gegen willkürliche Eingriffe durch die Behörden gegeben ist und ob ausreichende Garantien gegen Datenmissbrauch bestehen. Werden Daten gespeichert, gegen deren allfällige Verwendung kein zureichender Schutz gegen willkürliche Eingriffe durch die Behörden und keine ausreichenden Garantien gegen Datenmissbrauch bestehen, so ist dies konventionswidrig.

7.6. Die nationalen Instanzen haben demgegenüber argumentiert, zu prüfen sei nur die im BÜPF geregelte verwaltungsrechtliche Seite der Vorratsdatenspeicherung, nicht aber deren in der StPO geregelte strafprozessuale Seite (Ziff. 2. des angefochtenen Entscheids). Die nationalen Instanzen sind auf den Antrag, der Provider sei anzuweisen bzw. zu verpflichten, keine gespeicherten Verkehrs- und Rechnungsdaten der Beschwerdeführer an den Dienst ÜPF oder an andere Behörden oder an

Gerichte herauszugeben, nicht eingetreten. Es fehle an einem schutzwürdigen Interesse. Dies ist unrichtig, denn so lange Vorratsdaten gespeichert werden, droht auch deren Herausgabe an Behörden oder Gerichte. Ob eine solche Herausgabe während der laufenden rechtlichen Auseinandersetzung um die Vorratsdatenspeicherung stattfinden würde, können weder der Beschwerdeführer noch die nationalen Gerichtsinstanzen wissen, denn die Herausgabe würde (zumindest zunächst) heimlich erfolgen. Der entsprechende Antrag hätte somit behandelt werden müssen, damit die mit einer Herausgabe verbundenen Eingriffe in Konventionsrechte behandelt wird und deren Konventionswidrigkeit festgestellt werden kann. Indem die nationalen Instanzen diese Überprüfung unterlassen haben, haben sie den Beschwerdeführer in seinen in Art. 8 EMRK geschützten Ansprüchen verletzt und haben sein Recht auf effektive Beschwerde (Art. 13 EMRK) missachtet.
Unabhängig von der formellen Frage, ob und wie der soeben erwähnte Antrag der Beschwerdeführer zu behandeln gewesen wäre, muss bei der Beurteilung der Grundrechtskonformität der Datenspeicherung und der Schwere des damit verbundenen Eingriffs wie dargelegt notwendigerweise auch deren allfällige Verwendung durch Gerichte und Behörden einbezogen werden. Dies hängt mit der Behandlung des erwähnten Antrags nicht zusammen, würde also auch gelten, wenn dieser Antrag nicht gestellt worden wäre. Auch insofern ist Art. 8 EMRK und das Recht auf effektive Beschwerde (Art. 13 EMRK) missachtet worden.
7.7. Gemäss Praxis der Strassburger Organe muss die gesetzliche Grundlage bei Abhör- und Überwachungsmassnahmen in besonderem Masse konkret sein. Das Gesetz muss regeln, gegen wen die Abhörmassnahmen ergriffen werden, unter welchen Voraussetzungen, zum Schutz welcher Rechtsgüter, bei welchen Straftaten, mit welchen Mitteln und nach welchem Verfahren. Das Gesetz muss genügend konkret sein, so dass die Rechtsunterworfenen ermessen können, wie sie von der entsprechenden Überwachungsmassnahme betroffen sind. Dazu sind die Eingriffsmöglichkeiten durch die Regelung der Voraussetzungen und des Verfahrens so klar wie möglich zu umgrenzen. In verfahrensmässiger Hinsicht muss das innerstaatliche Recht ausreichend Schutz gegen willkürliche Eingriffe durch Behörden geben. Der Verweis in Art. 8 EMRK auf das nationale Recht in Zusammenhang mit der Betonung der demokratischen Gesellschaft beinhaltet die Notwendigkeit, die wesentliche Regelung in einer von ordentlichen Gesetzgeber (Parlament) erlassenen Regelung festgehalten ist und dass sich allfällige von der Exekutive erlassene Verordnungen auf eine entsprechende verfassungsrechtliche oder parlamentarische Ermächtigung stützen können. Es ist am Staat, zu belegen, dass die Eingriffe weder willkürlich noch ungesetzlich sind (vgl. Jens Meyer-Ladewig, Handkommentar EMRK, 3. Aufl., Baden-Baden 2011, Art. 8 Rn. 35 ff.; Frowein/Peukert, EMRK-Kommentar, 3. Aufl., Kehl am Rhein 2009, Vorbemerkungen zu Art. 8 Rn. 9); Annual Report oft he UN High Commis-

sioner for Human Rights, Navi Pillay, The right to privacy in the digital age, 30. Juni 2014 [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf] [wsEvents/Pages/DisplayNews.aspx?NewsID=14875&LangID=E]; Report of the Special Rapporteuron the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 7. April 2013 [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf]).

7.8. Die Vorratsdatenspeicherung in der Schweiz verfügt nicht über eine genügende gesetzliche Grundlage. Die effektive Praxis der Vorratsdatenspeicherung und der damit verbundene Eingriff in die Grundrechte wird für die Betroffenen aus den gesetzlichen Vorschriften nicht hinreichend klar. Das Gesetz selbst regelt die Vorratsdatenspeicherung nur in den Grundzügen. Die Regelung ist insgesamt zu abstrakt, als dass die Rechtsunterworfenen daraus ersehen könnten, wie die Vorratsdatenspeicherung in ihre Grundrechte eingreift.

7.9. Wie die Rechtsunterworfenen von der Vorratsdatenspeicherung betroffen sind, müsste sich schon aus dem Gesetz selbst (BÜPF) ergeben. Im Gesetz selber sind die Aufgaben des durchführenden Dienstes (Art. 13 BÜPF) und die Pflichten der Provider (Art. 15 BÜPF) nur rudimentär festgelegt. Der Bundesrat hat die VÜPF gestützt auf Art. 13 Abs. 3, Art. 15 Abs. 6 BÜPF festgelegt und es darin wiederum dem Dienst ÜPF überlassen, die technischen Details und Spezifikationen in Richtlinien unter Berücksichtigung der ETSI-Standards festzulegen (Art. 25 Abs. 4 VÜPF). Die genügt unter dem Aspekt der notwendigen demokratischen Legitimierung nicht, denn die VÜPF und die Richtlinien sind nicht vom Parlament erlassen worden und nicht dem fakultativen Volksreferendum unterstellt gewesen. Aus dem Gesetz erschliessen sich die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe nicht hinreichtend.

7.10. Die Schweizerische Praxis hat einschneidende Nutzungsmöglichkeiten von Vorratsdaten auf Verordnungsstufe oder gänzlich ohne konkrete generell-abstrakte Norm zugelassen, insbesondere die Rasterfahndung in gespeicherten Antennenstandorten samt Hauptstrahlrichtung von Mobiltelefonen (Antennensuchlauf), die Kopfschaltung, die Nutzung von Daten Tabellen von NAT-Routern und die Verwertung von gespeicherten Daten nach Ablauf von sechs Monaten, wenn diese beim Anbieter noch vorhanden sind. Hieraus ergeben sich exzessive Möglichkeiten zur Nutzung von Vorratsdaten, mit denen die Rechtsunterworfenen nicht rechnen.

7.11. Die Rechtfertigung und Notwendigkeit der Vorratsdatenspeicherung im Lichte der EMRK wäre von der Schweiz zu belegen und bei der Beurteilung durch die innerstaatlichen Gerichte zu überprüfen. Dazu gehört insbesondere, dass die Effektivität und Effizienz der Vorratsdatenspeicherung überprüft wird. Andernfalls kann die Voraussetzung der Notwendigkeit nicht

als erfüllt erachtet werden, und die Vorratsdatenspeicherung muss als konventionswidrig taxiert werden. Der Menschenrechtskommissar des Europarats hat sich in seinem Bericht vom 8. Dezember 2014 mit der Rechtmässigkeit der Europäischen Vorratsdatenspeicherung befasst. Darin gelangt er zum Schluss, die Speicherung sei als nicht effektiv zu bezeichnen, da keine signifikant positiven Effekte auf die Aufklärungsrate von Delikten zu verzeichnen seien (S. 115, u.a. mit Verweis auf Hans Jörg Albrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Max Planck Institute for Comparative and International Criminal Law, 2nd enlarged report, prepared for the German Federal Ministry of Justice, July 2011, at www.bmj.de/SharedDocs/Downloads/ DE/pdfs/20120127_MPI_ Gutachten_VDS_Langfassung.pdf?__blob=publicationFile) Der Menschenrechtskommissar hält die nationalen europäischen Gerichte ausdrücklich dazu an, die innerstaatlichen Gesetze über die Datenspeicherung auf ihre Effektivität und Effizienz zu überprüfen. Im Rahmen der Erforderlichkeit müsse sichergestellt werden, dass nur jene Bereiche der Datenspeicherung unterworfen werden, die eine solche Massnahme rechtfertigen. Die UNO hat sich ebenfalls mit der aktuellen Praxis der Massenüberwachung befasst, u.a. in den erwähnten zwei Berichten des Menschenrechtsrats der UNO Ein zentraler Aspekt dieser Berichte liegt darin, dass Menschenrechtseinschränkungen nur dann zulässig sein können, wenn der betreffende Staat die Notwendigkeit dieser Einschränkungen belegen kann.

7.12. Der Beschwerdeführer hat die Effektivität der Vorratsdatenspeicherung für die Aufklärung von Straftaten im nationalen Verfahren in Frage gestellt und den Verfahrensantrag gestellt, es sei die Praxis im Zusammenhang mit der Anordnung von Massnahmen zur rückwirkenden Überwachung des Fernmeldeverkehrs sowie deren richterlicher Überprüfung zu evaluieren. Die nationalen Instanzen sind weder diesem Antrag gefolgt, noch haben sie sonst die Effektivität der Vorratsdatenspeicherung überprüft oder auf irgend eine Art und Weise zu belegen vermocht. Die nationalen Instanzen führen als Beleg lediglich Gerichtsurteile an, in denen Konstellationen erwähnt wurden, in denen Vorratsdaten für die Aufklärung und die rechtliche Qualifikation des untersuchten Delikts von wesentlicher Bedeutung sein können. Eine solche anekdotische Berufung auf vorherige Gerichtsurteile stellt aber keine effektive Untersuchung der Notwendigkeit und Effektivität der Vorratsdatenspeicherung dar und vermag eine solche nicht zu ersetzen. Die Eignung der Vorratsdatenspeicherung kann durch eine solche abstrakte Argumentation nicht generell belegt werden. Der tatsächliche Beitrag der Vorratsdatenspeicherung zur Verbrechensaufklärung kann so nicht erfasst werden, und vor allen Dingen auch nicht deren Notwendigkeit. Mangels konkreter Untersuchung der Effektivität der Vorratsdatenspeicherung und

mangels weiterer Belege ist die Schweiz den Beleg schuldig geblieben, ob und in wie weit es für die Strafverfolgung tatsächlich notwendig ist, über die von der Vorratsdatenspeicherung erfassten Daten verfügen zu können. Indem die nationalen Instanzen nicht auf die entsprechenden Anträge und Vorbringen des Beschwerdeführers eingegangen sind, haben sie auch den Anspruch auf eine effektive Beschwerde gegen eine Konventionsverletzung verletzt (Art. 13 EMRK).

7.13. Der Menschenrechtskommissar des Europarats ist in seinem Bericht vom 8. Dezember 2014 zur Einschätzung gelangt, dass die Datenspeicherung mit den Grundsätzen der Rechtsstaatlichkeit nicht vereinbar ist. Er verweist dabei u.a. auf die Beurteilung der Vorratsdatenspeicherungsrichtlinie durch den EuGH. In den Urteilen vom 8. April 2014 und vom 21. Dezember 2016 ist der EuGH zum Ergebnis gelangt, dass die zu beurteilende Regelung der Vorratsdatenspeicherung die Grenzen des absolut Notwendigen überschreiten und nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann. Zulässig wäre eine Regelung, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist. Die betreffende nationale Regelung muss erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Massnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Massnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Massnahme auf das absolut Notwendige beschränkt wird. Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Massnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Massnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen. Bei der Begrenzung einer solchen Massnahme im Hinblick auf die potenziell betroffenen

Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden. Im Entscheid vom 8. April 2014 erklärte der EuGH die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten für ungültig, weil sich diese nicht auf das absolut Notwendige beschränke und somit unverhältnismässig sei. Dies begründete er unter anderem damit, dass sich die Richtlinie generell auf alle Personen, alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstrecke, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme vorzusehen. Insbesondere betreffe sie alle Personen, die elektronische Kommunikationsmittel benutzten, ohne dass diese auch nur mittelbar oder entfernt Anlass zur Strafverfolgung geben könnten. Auch verlange die Richtlinie keinen Zusammenhang zwischen den auf Vorrat gespeicherten Daten und der Bedrohung für die öffentliche Sicherheit. So beschränke sie sich weder auf Daten eines bestimmten Zeitraums, Gebiets oder eines Kreises von Personen, die in irgendeiner Weise in schwere Straftaten verwickelt sein oder aus anderen Gründen zur Verhütung oder Verfolgung solcher Delikte beitragen könnten. Zudem sehe die Richtlinie eine Mindestdauer von sechs Monaten für die Vorratsdatenspeicherung vor, ohne dass eine Unterscheidung der Datenkategorien je nach deren etwaigen Nutzen für das verfolgte Ziel oder anhand der betroffenen Personen getroffen werde (Urteil des EuGH vom 8. April 2014 C-293/12 und C-594/12 *Digital Rights Ireland*, Randnr. 57 ff.). Der EuGH bestätigte diese Rechtsprechung in seinem zweiten Urteil zur Vorratsdatenspeicherung (Urteil des EuGH vom 21. Dezember 2016 C-203/15 und C-698/15 *Tele2 Sverige*, Randnr. 108 ff.).

7.14. Der Menschenrechtskommissar hält im genannten Bericht ausdrücklich fest, dass die Daten nicht im Ausland gespeichert werden dürfen. Einzig aufgrund einer klaren, eindeutigen und hinreichend detaillierten internationalen Rechtsgrundlage, die den Anforderungen des Datenschutzes und anderen Menschenrechtsstandards genügt, könnte eine ausländische Speicherung rechtmässig erfolgen. Gleichzusetzen mit einer ausländischen Speicherung sei auch die Verbringung der Daten zum Speicherort über internationale Kabelwege (Commissioner for Human Rights, S. 21).

7.15. Der angefochtenen Regelung der Vorratsdatenspeicherung erfüllt die vorstehend dargelegten Voraussetzungen klar nicht. Es fehlt ihr auch

insoweit an der erforderlichen Notwendigkeit bzw. Verhältnismässigkeit. Auch die Vorgaben bezüglich Datenschutz und Schutz vor Datenmissbrauch, wonach die Art der Daten, die aufgezeichnet werden können, die Umstände, unter denen Überwachungsmassnahmen angeordnet werden dürfen, die Vorsichtsmassnahmen im Umgang mit aufgezeichneten Daten, die Zeitdauer der Aufbewahrung und das Verfahren für die Auswertung, Verwendung und Speicherung einschliesslich der Kreis der zugriffsberechtigten Personen und der Löschung der Daten im Gesetz selbst umschrieben sein müssen und wonach ein effektiver Schutz vor Missbrauch bestehen muss, sind nicht eingehalten. Der Zweck der Vorratsdatenspeicherung beschränkt sich nicht auf die Bekämpfung schwerer Straftaten. Es reicht grundsätzlich der Verdacht auf ein Verbrechen oder Vergehen, ein Delikt (Missbrauch einer Fernmeldeanlage) ist sogar nur eine Übertretung. Zahlreiche Delikte, welche als Vergehen ausgestaltet worden sind, können nicht als schwere Kriminalität bezeichnet werden, genügen jedoch in der Praxis als Anlassdelikt für die Vorratsdatenspeicherung. Auch Daten von nicht verdächtigten Personen können u.U. herausverlangt werden. Die Vorratsdatenspeicherung zielt auf alle Kommunikationsteilnehmer, welche über einen vom persönlichen Anwendungsbereich erfassten Provider eine vom sachlichen Anwendungsbereich erfasste Kommunikationsform nutzen, ohne dass diese auch nur mittelbar oder entfernt Anlass zur Strafverfolgung geben könnten. Insbesondere ist der gesamte Mobilfunkverkehr Gegenstand der Vorratsdatenspeicherung. Differenzierungen, Einschränkungen oder Ausnahmen fehlen weitgehend. Ein Zusammenhang zwischen den auf Vorrat gespeicherten Daten und der Bedrohung für die öffentliche Sicherheit ist nicht erforderlich. Die Speicherung beschränkt sich nicht auf Daten eines bestimmten Zeitraums, Gebiets oder eines Kreises von Personen, die in irgendeiner Weise in schwere Straftaten verwickelt sein oder aus anderen Gründen zur Verhütung oder Verfolgung solcher Delikte beitragen könnten. Die Daten bleiben uneingeschränkt für die Dauer von sechs Monaten gespeichert. Es liegt keine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vor, welche sich diese hinsichtlich der Datenkategorien, der elektronischen Kommunikationsmittel, des Personenkreises und der Aufbewahrungsdauer auf das absolut Notwendige beschränkt. Sie ist nicht auf objektive Anhaltspunkte gestützt, die es ermöglichten, diejenigen Personen zu erfassen, die einen zumindest mittelbaren Zusammenhang zu schweren Straftaten aufwiesen, etwa, indem eine Begrenzung durch ein geografisches Kriterium gewährleistet wäre, bezogen auf objektive Hinweise dafür, dass in gewissen Gebieten ein erhöhtes Risiko für die Vorbereitung oder Begehung von Straftaten besteht. Dass die entsprechenden Daten aller Provider gespeichert werden, fällt auch vor dem Hintergrund einiger weitreichender Nutzungsmöglichkeiten ins Gewicht (insbesondere Antennensuchlauf, Kopfschaltung, Nutzung von Daten aus Tabellen von NAT-Routern und die Verwertung von allenfalls auch nach Ablauf von sechs

Monaten noch vorhandenen Daten). Beim Antennensuchlauf und bei der Kopfschaltung können zahlreiche Personen in eine Strafverfolgung einbezogen werden, ohne dass gegen diese ein Tatverdacht bestünde oder sie sonst selbst einen konkreten Anlass dafür gegeben hätten, und ohne dass sie darüber informiert werden. Der angefochtenen Regelung fehlt es damit an der erforderlichen Notwendigkeit.

7.16. Das Bundesgericht stellt diesen Befund in seinem Entscheid nicht in Abrede. Es führt lediglich Zweifel an der Praktikabilität einzelner vom EuGH vorgesehener Einschränkungen ins Feld und argumentiert im Übrigen, das Wesen der Vorratsdatenspeicherung bestehe gerade darin, die von den Benutzern von Fernmeldediensten bei ihren Kommunikationsvorgängen generierten äusseren Daten über eine gewisse Zeitspanne zu erhalten, ohne zu wissen, ob sie für eine allfällige künftige Strafuntersuchung von Bedeutung sein werden oder nicht. Der schweizerische Bundesgesetzgeber habe sich ausdrücklich für dieses System der umfassenden und anlasslosen Speicherung und Aufbewahrung von Randdaten der Telekommunikation ausgesprochen und diesen Entscheid im Rahmen der Totalrevision des BÜPF bestätigt und die Einführung des von den Beschwerdeführern als mildere Massnahme vorgeschlagenen "quick freeze"-Verfahrens explizit verworfen. Dieses falle als weniger weitreichende Massnahme ausser Betracht, zumal es eine geringere Zwecktauglichkeit aufweise als das geltende System und somit nicht den vom Gesetzgeber erwünschten Erfolg zu zeitigen vermöge. Das Bundesgericht bringt zur Rechtfertigung der anlasslosen Speicherung von Randdaten also lediglich vor, dass sich die Schweiz bewusst für diese entschieden habe und dass eine weniger weit gehende Lösung den damit verfolgten Zweck weniger gut zu erfüllen vermöchte. Dass sie die vorstehend dargelegten konventionsrechtlichen Anforderungen nicht erfüllt, räumt das Bundesgericht damit implizit ein.

7.17. Es ist auch daran festzuhalten, dass das als «quick freeze» bezeichnete Verfahren einen kleineren Grundrechtseingriff darstellt und als ausreichend erscheint. Bei diesem Verfahren werden vorhandene Metadaten sofort gesichert, sobald ein dringender Tatverdacht vorliegt. Kurze Zeit später kann entschieden werden, in wie weit ein Anfangsverdacht Anlass gibt, die gesicherten Daten in einem konkreten Strafverfahren zu verwenden. Der grosse Unterschied ist hierbei, dass – wie bei anderen Zwangsmassnahmen auch – erst der dringende Tatverdacht überhaupt Anlass für den Grundrechtseingriff gibt. Dagegen erleiden bei der Vorratsdatenspeicherung alle an der Kommunikation mit Post und Fernmeldeverkehr teilnehmenden Personen einen Eingriff in die Grundrechte, was nicht als notwendig erscheint. Aus den vom Dienst ÜPF geführten Statistiken ersichtlich ist, dass die Strafverfolgungsbehörden in den meisten Fällen nur zeitnah angefallene Daten benötigen, was gegen die Notwendigkeit einer allgemeinen Aufbewahrungsdauer von sechs Monaten spricht (vgl. Medienmitteilung der SwiNOG Federation vom 16. Juni 2013, https://www.digitale-

gesellschaft.ch/2013/06/13/neue-statistiken-vorratsdatenspeicherung-ist-auch-hinsichtlich-der-vorhaltedauer-unverhaltnismassig/).

8. (ad Art. 10 und Art. 13 EMRK)

8.1. Der Beschwerdeführer hat als Journalist vorgebracht, dass die Vorratsdatenspeicherung den Quellenschutz und die Medienfreiheit verletzt. Die nationalen Instanzen haben sich damit nicht im Einzelnen befasst, sondern sich im Wesentlichen auf das Argument beschränkt, es sei nicht nötig, dies eingehend zu prüfen, zumal die Frage, ob die Strafprozessordnung diesbezüglich einen hinreichenden Schutz bietet, nicht vom Streitgegenstand erfasst werde (E 1.2). Dies wird den vom Beschwerdeführer erhobenen Rügen und dem Grundrechtseingriff, welchen er durch die Vorratsdatenspeicherung erleidet, nicht gerecht. Der Beschwerdeführer hat geltend gemacht, dass er bereits durch die Vorratsdatenspeicherung an sich im Anspruch auf Quellenschutz und in der Medienfreiheit verletzt ist. Die Frage, in welcher Art und Weise er als Journalist durch die Vorratsdatenspeicherung betroffen ist, kann nicht losgelöst von der potenziellen Verwendung der Daten im Rahmen eines Strafprozesses beurteilt werden, zumal der Beschwerdeführer dargelegt hat, dass die Wahrung der entsprechenden Grundrechte im Strafprozess eben nicht gewährleistet ist.

8.2. Wenn es in einem allfälligen Strafprozess dazu kommen kann, dass der Quellenschutz durchbrochen wird, wenn m.a.W. keine zuverlässigen strafprozessualen Mechanismen bestehen, welche garantieren können, dass der Quellenschutz bei der Verwendung von Vorratsdaten gewahrt bleibt, dann kann der Quellenschutz nur gewährleistet werden, wenn zum Vornherein keine dem Quellenschutz unterliegenden Vorratsdaten erfasst werden. Es ist deshalb nicht möglich, den Schluss zu ziehen, der Quellenschutz des Beschwerdeführers sei durch die Vorratsdatenspeicherung nicht verletzt, ohne sich inhaltlich mit der strafprozessualen Seite der Vorratsdatenspeicherung zu befassen, also ohne zu prüfen, ob die strafprozessualen Bestimmungen die Verletzung des Quellenschutzes bei der Verwendung von Vorratsdaten zu verhindern vermögen. Mit der Frage, ob der Antrag der Beschwerdeführer, der Anbieter sei anzuweisen, keine ihn betreffenden Daten zu speichern, zu behandeln ist, hat dies im Übrigen nichts zu tun, denn die Verletzung des Quellenschutzes liegt bereits in der Speicherung von Vorratsdaten, welche einen Journalisten betreffen, an sich. Wenn die strafprozessualen Garantien zur Wahrung des Quellenschutzes nicht genügen, so kann der Journalist auch nicht auf die Möglichkeit verwiesen werden, den Quellenschutz in einem allfälligen Strafprozess geltend zu machen und durchzusetzen, denn aufgrund der ungenügenden strafprozessualen Garantien wird er auf diese Weise nicht erfolgreich sein und die Verletzung des Anspruchs auf Quellenschutz nicht abwenden können.

8.3. Wie im Sachverhalt dargelegt garantieren die in der StPO vorgesehenen Schutzbestimmungen keinen wirksamen Quellenschutz. Die Bestimmungen vermögen nicht wirksam zu verhindern, dass Vorratsdaten, welche dem Quellenschutz unterliegen, den Strafverfolgungsbehörden bekannt werden. Soweit es sich beim Kommunikationspartner um eine geschützte Quelle handelt, liegt die entsprechende Information den Strafverfolgungsbehörden mit der Einholung der Auskunft über die Vorratsdaten unmittelbar vor. Alle Mechanismen, welche danach sicherstellen sollen, dass der Quellenschutz gewahrt bleibt, vermögen dies nicht wirksam sicherzustellen. Die Durchsetzung der vorgesehenen Aussonderung und Unverwertbarkeit nach Art. 271 Abs. 3 StPO würde im Falle eines Journalisten voraussetzen, dass die Behörde, welche die Aussonderung vornimmt und sich der Unverwertbarkeit bewusst sein soll, gerade davon Kenntnis hat, dass es sich um eine Quelle handelt, womit das Wissen, wer die Quelle des Journalisten ist, bereits in die Köpfe der damit befassten Strafverfolgungsbehörden gelangt ist. Es besteht das unlösbare Grundproblem, dass die Berücksichtigung des Quellenschutzes bei Vorratsdaten, welche zu den Strafverfolgungsbehörden gelangt sind, regelmässig voraussetzt, dass sich das Gericht oder die Strafverfolgungsbehörde der Tatsache bewusst sind, dass Daten vorliegen, welche auf den Kontakt zwischen einem Journalisten und seiner Quelle hinweisen. Genau das Vorhandensein dieser Information bzw. die Kenntnis von Gericht und Behörden darüber vereitelt jedoch den Quellenschutz und verletzt den Anspruch auf Gewährleistung des Quellenschutzes.

8.5. Es bestehen damit keine wirksamen Schutzmechanismen gegen die mit der Vorratsdatenspeicherung verbundene Kompromittierung des Quellenschutzes. Der Journalist muss damit rechnen, dass Vorratsdaten, die durch die Kommunikation mit Quellen anfallen, in einem Strafverfahren beigezogen werden und so seine Quellen offen legen. Der Quellenschutz ist damit durch die Vorratsdatenspeicherung beeinträchtigt und kann nicht mehr garantiert werden, sobald der Journalist Kommunikationsmittel verwendet, die der Vorratsdatenspeicherung unterliegen. Die mit der Vorratsdatenspeicherung verbundenen Einschränkungen der Grundrechte wiegen damit für den Beschwerdeführer besonders schwer, einschliesslich des darin enthaltenen «chilling effects». Die Vorratsdatenspeicherung beeinträchtigt damit seine Arbeit bzw. seine Arbeitsweise nachhaltig, zumal er als Journalist eigentlich essenziell auf Kommunikation und die Nutzung zeitgemässer Kommunikationskanäle angewiesen ist. Der Journalist steht vor der Wahl, sich bei der Kommunikation, die der Vorratsdatenspeicherung unterliegt, vom Quellenschutz zu verabschieden, oder aber, diese Kommunikationsformen nicht mehr zu nutzen. Der Anspruch auf Quellenschutz und auf Medienfreiheit ist damit verletzt.