The Data Retention Directive

Lukas Feiler
Matrikelnummer: 0201227

European and International Technology Law Seminar:
Intellectual Property Rights, Information Technology Law,
Biotechnology Law

Supervisor: ao.Univ.-Prof. Dr. Siegfried Fina
Submitted on: 2 May 2008

Table of contents

1. Introduction....1
2. The personal scope of the obligation to retain data....2
3. Transposition of the Directive....4
4. Data to be retained....4
   4.1. General limitations....4
   4.2. Traffic data categories and affected means of communication....5
5. The minimum and maximum retention periods....9
6. Access to retained data....9
7. Legality of the Directive with regard to European fundamental rights....10
   7.1. Interference with the right to privacy....10
   7.2. “In accordance with the law”....12
   7.3. “Necessary in a democratic society" for a recognized purpose....13
      7.3.1. The public purpose of the Directive....13
      7.3.2. Suitability....13
      7.3.3. Necessity....14
      7.3.4. Proportionality....15
      7.3.4.1. Effectiveness with respect to the Directive’s objective....15
      7.3.4.2. Severity of the interference....22
      7.3.4.3. Adequate and effective measures against abuse....25
      7.3.4.4. Conclusion....26
8. Legality of the Directive with regard to the competences of the EC....28
   8.1. The aim of the Directive....29
   8.2. The content of the Directive....30
   8.3. A comparison with C-317/04 (passenger name records)....31
   8.4. Conclusion....32

Bibliography....34

Abstract

The Data Retention Directive (2006/24/EC) provides the obligation for providers of publicly available electronic communications services or of public communications networks to retain traffic and location data for six months up to two years for the purpose of the investigation, detection and prosecution of serious crime. Considering potential uses and misuses of retained data such as traffic analysis, social network analysis and data mining, this paper examines the suitability, necessity and proportionality of the interference with the right to privacy posed by the Directive. Taking into account recent case law it also discusses the critical question of whether the European Community had any competence under Art 95 EC to issue the Directive.

1. Introduction

The Data Retention Directive (hereinafter referred to as the Directive)[1] marks a departure from European data protection principles as they have been established by the Directives 95/46/EC[2] and 2002/58/EC[3].

After the acts of terrorism committed on 9/11, in 2004 in Madrid and in 2005 in London the political climate – at least to some extent based on an emotionally perceived high level of risk – allowed for (or even demanded) drastic measures.[4] The Directive certainly fits that bill.

This paper will focus on the question of the legality of the Directive, specifically the interference with the right to privacy and the competence of the European Community

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. All unqualified Articles and Recitals used in this text refer to this Directive.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[4] For a general discussion of the conflict between privacy and the fight against crime and terrorism, see *Benn-Ibler*, Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten, AnwBl 2008, 12. For a more international perspective, see *Warner*, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, University of Ottawa Law & Technology Journal, Vol. 2, No. 1 (2005), 75.

under Art 95 EC to issue the Directive. As much has already been written about the turbulent legislative history[5] of the Directive, this paper will only refer to it where necessary to construe provisions of the Directive.

2. The personal scope of the obligation to retain data

Art 3 states that only "providers of publicly available electronic communications services" and providers of "public communications networks" are obligated to retain any data. Art 2(1) refers to the definitions provided by 2002/21/EC[6].

Art 2(c) 2002/21/EC defines the term "electronic communications service" as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks". "[S]ervices providing, or exercising editorial control over, content transmitted using electronic communications networks and services" are explicitly excluded. In the context of the Directive, the most important question is whether only Internet access providers or also other providers (like mail service providers) provide an "electronic communications service". Art 2(c) 2002/21/EC requires that the service wholly or mainly consists "in the conveyance of signals on electronic communications networks". With respect to the Internet this definition only matches Internet access providers. Their service consists in the "conveyance of signals" without any editorial control. Technically speaking, they provide services on the first three layers of the OSI networking model[7]: the physical layer, the data link layer and the network layer[8].

Services provided *over* the Internet (as opposed to service providing *access to* the Internet) do not mainly consist "in the conveyance of signals" – that is something left to Internet access providers. Services provided over the Internet use the last (or topmost) four layers of the OSI networking model: the application layer, the presentation layer, the session

[5] See *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 7 et seq; *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34 et seq.

[6] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[7] Open Systems Interconnection model, see ISO/IEC 7498; *Harris*, CISSP All-in-One Exam Guide³ (2005) 417 et. seq.

[8] These three OSI layers correspond to the following layers in the TCP/IP networking model: the link layer (e.g. Ethernet) and the network layer (e.g. IP, ICMP and IGMP). See *Stevens*, TCP/IP Illustrated, Volume 1 (1994), 2.

layer and the transport layer[9]. They do not concern themselves with the first three layers of the OSI networking model, i.e. with the "conveyance of signals".

Recital 10 2002/21/EC seems to contradict Art 2(c) 2002/21/EC when it states that "Voice telephony and electronic mail conveyance services are covered by this Directive". But the term "conveyance" as it is used in Recital 10 2002/21/EC is to be understood in the same context as it is used in Art 2(c) 2002/21/EC. The person conveying an e-mail or a signal is not the one who initiates its transmission but rather the one who actually performs the conveyance. It is not the mail service provider but rather its Internet access provider who conveys an e-mail (using signals on electronic communications networks).

Mail service providers provide their service *over* the Internet and are therefore not "providers of publicly available electronic communications services" as referred to in Art 3 of the Directive.

A similar question is raised with regard to providers of Internet telephony services.[10] Here it is necessary to differentiate between a VoIP service provided entirely over the Internet and a service that also allows its users to call into or receive calls from the mobile or fixed telephone network.[11] In the former case the VoIP provider entirely relies on Internet access providers to convey the actual signals on the electronic communications network. In the latter case the VoIP provider's service does consist of conveying signals on the telephone network. From a functional perspective an Internet telephony provider acts as an Internet access provider when a call is placed from the telephone network to a VoIP user and as a telephone network access provider when a VoIP user places a call into the telephone network. Therefore only VoIP providers that allow access to or from the telephone network can be considered "providers of publicly available electronic communications services" as referred to by Art 3 of the Directive.

---

[9] These four OSI layers correspond to the following layers in the TCP/IP networking model: the transport layer (TCP or UDP) and the application layer (e.g. HTTP, SMTP, FTP). See *Stevens*, TCP/IP Illustrated, Volume 1 (1994), 2.

[10] For an introduction to VoIP and network convergence, see *Analysys*, Final Report for the European Commission: IP Voice and Associated Convergent Services (2004).

[11] See, inter alia, *Gschweitl/Langmantel/Reichinger*, Voice over IP - Rechtliche Einordnung eines neuen Konzeptes, MR 2005, 503.

The second kind of providers named in Art 3 are providers of "public communications networks". Art 2(d) 2002/21/EC defines the term "public communications network" as "an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services". Art 2(a) 2002/21/EC further defines the term "electronic communications network" as "transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals […] by […] electromagnetic means […]". A provider of "public communications networks" as referred to by Art 3 therefore is the person who provides the network infrastructure that permits the conveyance of signals.

3. Transposition of the Directive

Art 15(1) states that the Member States have to implement the Directive by 15 September 2007. According to Art 15(3) Member States may also postpone the Directive's implementation until 15 March 2009 but only with regard to Internet access, Internet e-mail and Internet-telephony.[12] Sixteen Member States chose to do so.

4. Data to be retained

4.1. General limitations

Art 3(1) states that providers of publicly available electronic communications services or of public communications networks only have to retain data that they "generated or processed".[13] As Art 2(1) refers to 95/46/EC with regard to the definitions contained therein, the term "processed" has to be construed according to Art 2(b) 95/46/EC which defines "processing of personal data" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means […]". All data (re)transmitted by a provider therefore is "processed".

The requirement that the data has to be "generated or processed" makes clear that the providers have no obligation to generate new data, for example by requiring their users to provide personal data, such as a social security number to buy a pre-paid cell phone.

[12] See, inter alia, *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 54.
[13] See, inter alia, *Otto/Seitlinger*, Die „Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, 231.

Recital 13 explicitly states that the data to be retained has to be "accessible". It further notes with regard to Internet e-mail and Internet telephony that the obligation to retain data may apply only in respect of data "from the provider's or the network providers' own services". As the Directive only covers "publicly available electronic communications services" the term "service" as it is used in Recital 13 is to be construed in that sense.[14]

A further limitation is provided by Art 5(2) which states that "[n]o data revealing the content of the communication may be retained pursuant to this Directive". As discussed below, traffic data if professionally analyzed will necessarily reveal at least parts of or hints to the contents of a communication.[15] A simple example would be regular calls to a cardiologist only occurring during office hours. Art 5(2) therefore seems to essentially contradict Art 5(1). To resolve this contradiction one has to interpret the phrase "data revealing the content" in Art 5(2) as data "containing" or "directly revealing" the content. This can also be supported by the last sentence of Art 1(2) which states that "[the Directive] shall not apply to the content of electronic communications". This means that Art 5(2) only emphasizes what is obvious from Art 5(1): the content of communications must not be retained pursuant to the Directive.[16]

4.2. Traffic data categories and affected means of communication

Art 5(1) names six categories of data to be retained: (a) data necessary to trace and identify the source of a communication; (b) data necessary to identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify users' communication equipment or what purports to be their equipment and (f) data necessary to identify the location of mobile communication

[14] Of a different opinion, *Otto/Seitlinger*, Die „Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, 233; they appear to read Recital 13 in a way that providers of publicly available electronic communications services or of public communications networks are only obligated to retain data with respect to Internet e-mail and Internet telephony services they offer themselves. Unless one regards all mail and VoIP service providers obligated to retain data – which they apparently do – this would effectively render the Directive useless with respect to Internet e-mail and Internet telephony.
[15] See, inter alia, *Gitter/Schnabel*, Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411, 414.
[16] See, inter alia, *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 15.

equipment. This broad list of categories is considerably limited by the means of communication to which they apply.

According to Art 5(1) traffic data is only to be retained in relation to five specific means of communication: fixed network telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. The kind of traffic data to be retained for each means of communication shall now be discussed.[17]

When fixed network telephony or mobile telephony is used for communication the telephone number, name, address[18] of the caller and the callee(s), the date and time of the start and end of the communication[19], and the type of telephone service used[20] are to be retained. For mobile telephony the caller and the callee(s) IMSI[21], IMEI[22] and cell ID[23] also have to be retained at the start of the communication. In the case of pre-paid anonymous mobile telephony services the date and time of the initial activation and the cell ID from which the activation occurred also have to be retained. The data relating to unsuccessful call attempts does not have to be retained.[24]

With regard to Internet access the following data has to be retained: the allocated IP address[25], user ID(s)[26], the calling telephone number in case of dial-up access[27], the name

[17] The structure of Art 5(1) is based on the six different categories instead of the five means of communication. The author finds the latter approach more practical as it allows a better understanding of the data actually retained when using a certain means of communication.
[18] Art 5(1)(a)(1) and Art 5(1)(b)(1). According to Art 5(1)(b)(1)(i) this may include multiple telephone numbers per callee if call forwarding is used.
[19] Art 5(1)(c)(1).
[20] According to Art 2(2)(c) this may be a call (including voice, voicemail, conference and data calls), a supplementary service (including call forwarding or call transfer) or a messaging or multi-media service (including a short message service, an enhanced media service or a multimedia service).
[21] International Mobile Subscriber Identity. It identifies the SIM card; see ITU-T Recommendation E.212, The international identification plan for mobile terminals and mobile users, http://www.itu.int/rec/T-REC-E.212-200405-I/en.
[22] International Mobile Equipment Identity. It identifies a mobile phone itself.
[23] While the wording of Art 5(1)(f) is unclear as to whose cell ID is to be retained Art 2(2)(e) defines a cell ID as a "the identity of the cell from which a mobile telephony call originated or in which it terminated". According to Art 5(1)(f)(2) data identifying the geographic location of cells also has to be retained.
[24] However, Art 2(2) explicitly allows the Member States to mandate the retention of data with respect to unsuccessful call attempts. Unsuccessful call attempts have been the subject of much debate. See *Benn-Ibler*, Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten, AnwBl 2008, 12, 14; Westphal, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 36.
[25] Contrary to common sense, the obligation to retain the assigned IP address is to be found in Art 5(1)(c) and not Art 5(1)(a).

and address of the person to whom the IP address was allocated[28], the date and time of the log-in and log-off[29] and the DSL or other end point (on the user's side)[30]. In the case of mobile Internet access, the cell ID – along with data identifying the geographic location of the cell – also has to be retained "at the start of the communication", i.e. when the Internet connection is established. It has to be emphasized that no data with regard to Internet access is to be retained "to identify the destination of a communication" (Art 5(1)(b)) or "to identify the type of communication (Art 5(1)(d)).[31] With regard to Internet e-mail and Internet telephony, "Internet access" therefore is not a subsidiary "catch-all" means of communication.

With regard to Internet e-mail the sender's and the recipient's e-mail addresses ("user IDs")[32], telephone numbers in case of dial-up access[33], DSL or other end points (on the user's side)[34], names and addresses[35] are to be retained. To identify the date, time and duration of the communication, Art 5(1)(c)(2)(ii) states that the "date and time of the log-in and log-off of the Internet e-mail service" has to be retained. This wording raises serious problems. The sending of an e-mail does not necessarily commence with the log-in and also does not necessarily complete with the log-off. A user could use a single log-in session to send and/or receive multiple e-mails over a considerable time span. In an effort to craft a single provision that would cover Internet e-mail and Internet telephony the European legislator seems not to have considered this fact. But as the wording of Art 5(1)(c)(2)(ii) is clear, not the point in time an e-mail was actually sent or received but

---

[26] Art 2(2)(d) defines a user ID as a unique identifier allocated to persons when they subscribe to or register with the service in question. This could be a username when using a dial-up Internet connection.
[27] Art 5(1)(e)(3)(i) explicitly mentions "dial-up access".
[28] Art 5(1)(a)(2)(iii).
[29] Art 5(1)(c)(2)(i).
[30] Art 5(1)(e)(3)(ii) uses the phrase „end point of the originator of the communication" to achieve applicability for Internet access, Internet e-mail and Internet telephony. With regard to Internet access the "originator of the communication" clearly is the user as he initiates the internet connection.
[31] See, inter alia, *Gitter/Schnabel*, Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411.
[32] Art 5(1)(a)(2)(i) and Art 5(1)(b)(2)(ii).
[33] Art 5(1)(e)(3)(i).
[34] Art 5(1)(e)(3)(ii) uses the phrase „end point of the originator of the communication". In the context of Internet e-mail this could be read as only to refer to the sender of the e-mail. But this provision has to be read in context with the preceding Art 5(1)(e)(3)(i) which mentions the "calling telephone number" in the context of Internet access, Internet e-mail and Internet telephony. The "originator" of the communication in Art 5(1)(e)(3)(ii) therefore has to be understood as a caller in terms of Art 5(1)(e)(3)(i). Art 5(1)(e)(3)(ii) can therefore apply to both, the sender and the recipient of an e-mail.
[35] Art 5(1)(a)(2)(iii); Art 5(1)(b)(2)(ii).

the log-in and log-off time of the Internet e-mail service has to be retained. The Directive does not define the term "Internet e-mail service". The term certainly covers services offered using the standardized e-mail protocols SMTP[36], POP3[37] and IMAP[38].[39] To identify the type of communication information about "the Internet service used" has to be retained. The Directive does not provide a definition for the term "Internet service". Art 2(2)(c) defines "telephone service" as the type of service and not as a specific service offered by a specific provider. "Internet service" is therefore to be construed as to mean the type of mail service (e.g. SMTP, POP3 or IMAP) and not the IP address and port number of the actual service used (e.g. 216.139.219.28:25). If mobile equipment is used to send and/or receive mails the cell ID (along with data identifying the geographic location of the cell) has to be retained "at the start of the communication". As each individual e-mail has to be considered a "communication" in its own right, the cell ID has to be retained for every e-mail sent from or received by a mobile device.

In the case of Internet telephony the following data has to be retained: the caller's and the callee's VoIP addresses[40] ("user IDs")[41], names and addresses[42]; in case of a VoIP-to-telephone-network-call the callee's telephone number and the telephone number assigned to the caller[43], telephone numbers in case of dial-up Internet access[44], DSL or other end points (on either user's side)[45], the date and time of the log-in and log-off of the Internet telephony service and the type of Internet service used. "Internet service" in the context of VoIP could be construed as to mean which VoIP protocol (e.g. SIP) was used. If mobile equipment is used to perform the VoIP communication, the cell ID (along with the data

[36] *Klensin*, RFC 2821, Simple Mail Transfer Protocol (2001).
[37] *Myers/Rose*, RFC 1939, Post Office Protocol - Version 3 (1996).
[38] *Crispin*, RFC 3501, Internet Message Access Protocol - Version 4Rev1 (2003).
[39] See below for a discussion of alternative mail transfer protocols, including web mail.
[40] *Rosenberg/Schulzrinne* et al., RFC 3261, SIP: Session Initiation Protocol (2002), Section 19.1.3; *Wallingford*, Switching to VoIP (2005), 150.
[41] Art 5(1)(a)(2)(i) and Art 5(1)(b)(2)(i).
[42] Art 5(1)(a)(2)(iii); Art 5(1)(b)(2)(ii). As the term "communication" is used in Art 5(1)(b)(2)(ii), it applies to both, Internet e-mail and Internet telephony.
[43] Art 5(1)(a)(2)(ii); when calling "out" (from the Internet to the telephone network) the caller is sometimes assigned a temporary telephone number. This is why the phrase "telephone number allocated to any communication entering the public telephone network" was chosen for Art 5(1)(a)(2)(ii).
[44] Art 5(1)(e)(3)(i).
[45] Art 5(1)(e)(3)(ii).

identifying the geographic location of the cell) has to be retained at the start of the communication.[46]

5. The minimum and maximum retention periods

Art 6 states that the data specified in Art 5 is to be retained "for periods of not less than six months and not more than two years of the date of the communication". The first issue to be considered is a rather practical one: how often to search for data old enough to have to be deleted? Art 6 uses the wording "date of the communication". This indicates that traffic data exceeding the retention period set by a Member State only has to be deleted once a day.

Art 6 gives the Member States considerable flexibility in determining the retention period. Adding to this flexibility is Art 12[47]. It allows Member States "facing particular circumstances" to extend the retention period. Said circumstances have to warrant such an extension and the extension itself may only be valid for a limited period. The Member State has to inform the Commission and other Member States immediately. According to Art 12(2) the Commission has the power to approve or reject the extension. If it does not act until six months after the notification the extension is deemed to have been approved.

It finally is important to reiterate that the limits for the retention period only affect data that is to be retained in accordance with Art 5. The Directive therefore does not establish a general maximum data retention period.

6. Access to retained data

Art 4 states that traffic data retained in accordance with the Directive shall be "provided only to the competent national authorities in specific cases and in accordance with national law". But as Recital 25 reiterates, the Community has no power to regulate the issue of access by national authorities for activities referred to in the first indent of Art 3(2) 95/46/EC. These include activities provided for by Titles V and VI EU and "processing

[46] Art 5(1)(f)(i) and (ii).

[47] See *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 37; *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 52; *Gitter/Schnabel*, Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411, 412.

operations concerning public security, defence, State security […] and the activities of the State in areas of criminal law".[48]

When interpreting Art 4 in the light of Recital 25 it becomes clear that the Directive sets no limits whatsoever on the conditions or kind of access a Member State may grant a national authority to the retained data. The same holds true for Art 1 that states that the retention is to be performed, "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law".[49]

But as the Community does have the power to regulate all access by actors that are not national authorities, Art 4 e contrario provides that the retained data must not be provided to private entities.

7. Legality of the Directive with regard to European fundamental rights

When determining the legality of the Directive with regard to European fundamental rights it is important to keep in mind that the Directive itself does not state the conditions under which access to the retained data may be granted.

7.1. Interference with the right to privacy

Art 6(2) EU states that the European Union shall respect fundamental rights as general principles of Community law. According to Art 6(2) EU, said fundamental rights are to be derived from the European Convention for the Protection of Human Rights and Fundamental Freedoms[50] and from the constitutional traditions common to the Member States[51]. As all Member States have ratified[52] the Council of Europe Convention 108[53] it might be used to determine common constitutional traditions. The Charter of Fundamental

[48] See, inter alia, ECJ 20.5.2006, C-317/04.
[49] *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 53; not considering Recital 25 and of a contrary opinion, *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 19 et seq. and *Bignami*, European versus American liberty: A comparative privacy analysis of antiterrorism data mining (2007) 609, 655.
[50] Hereinafter referred to as ECHR.
[51] See, in particular, ECJ 6.3.2001, C-274/99 P, § 37; ECJ 18.6.1991, C-260/89, § 41.
[52] See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG.
[53] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaties No. 108 (28.1.1981).

Rights of the European Union is not legally binding and therefore might only provide some level of guidance when interpreting the common constitutional traditions. Specifically the Charter provides for the protection of personal data in Art 8 and the respect for private and family life in Art 7.

Art 8 § 1 ECHR stipulates everybody's right "to respect for his private and family life, his home and his correspondence"[54]. The European Court of Human Rights established in Klass[55] that telephone communications fall under both "correspondence" and "private life".[56] The Court has further held in Malone[57] that not just the contents of telephone communications but also the telephone numbers dialed (i.e. traffic data) are protected under Art 8 ECHR. In Copland[58] the court held that this principle also applies to e-mail communication.

As the Directive does not regulate the conditions under which access may be granted to the retained data, the issue arises whether the data retention in itself constitutes an interference with the right to privacy. The European Court of Human Rights stated in Amann that "the storing of data relating to the 'private life' of an individual falls within the application of Article 8 § 1 [ECHR]"[59]. Citing this principle, the Court further elaborated in Copland that "it is irrelevant that the data held […] were not disclosed or used […] in disciplinary or other proceedings".[60] The right to privacy as it is provided by Art 8 ECHR is therefore to be understood in a very broad sense. One can therefore derive from Art 8 ECHR a general principle of Community law that provides an extensive right to privacy with respect to personal data. This general principle also finds support in the Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and in the Council of Europe Convention 108.

[54] See, inter alia, ECJ 20.5.2003, C-465/00, C-138/01 and C-139/01, § 68 et seq.
[55] E.C.H.R. 6.9.1978, Klass and Others v. Germany, Ser. A no. 28, § 41.
[56] See, inter alia, *Frowein* in *Fowein/Peukert*, Europäische Menschenrechtskonvention² (1996), Artikel 8, §§ 6, 34.
[57] E.C.H.R. 2.8.1984, Malone v. The United Kingdom, Ser. A no. 82, § 84.
[58] E.C.H.R. 3.4.2007, Copland v. The United Kingdom, § 43.
[59] E.C.H.R. 16.2.2000, Amann v. Switzerland, ECHR 2000-II, § 65, referring to E.C.H.R. 26.3.1987, Leander v. Sweden, Ser. A no. 116, § 48.
[60] E.C.H.R. 3.4.2007, Copland v. The United Kingdom, § 43.

The retention of traffic data by itself therefore constitutes an interference with the right to privacy as it is provided by Art 8 ECHR. As the retention is mandatory, the Directive does not leave the member states the possibility to implement the directive in a way that would not interfere with the right to privacy. The Directive itself therefore has the potential to violate the general principle of the right to privacy.

Art 8 § 2 ECHR states that an interference with the exercise of the right conferred by Art 8 § 1 ECHR is only permissible if it is "in accordance with the law" and "necessary in a democratic society" for a recognized purpose.

7.2. "In accordance with the law"

The European Court of Human Rights has repeatedly held that the phrase "in accordance with the law" in Art 8 § 2 ECHR also relates to the quality of the law and does not only refer back to domestic law.[61] Said quality has to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention.

Art 5 of the Directive uses a very complex approach to define the specific types of traffic and location data to be retained. As described above it does not deal with each type of communication (fixed network telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony) separately. It rather deals with all types of communication under each of the six data categories. In an effort to use the same wording for multiple types of communication Art 5 also ignores certain technical facts[62] and thereby specifies the data to be retained less precisely than intended.

But with sufficient technical understanding of the communication technologies involved all terms used in Art 5 can be applied to the five types of communication in a way that foreseeability[63] can be established with respect to what data will be retained.

---

[61] E.C.H.R. 2.8.1984, Malone v. The United Kingdom, Ser. A no. 82, § 67; E.C.H.R. 16.2.2000, Amann v. Switzerland, ECHR 2000-II, § 56; E.C.H.R. 4.5.2000, Rotaru v. Romania, ECHR 2000-V, § 55.

[62] As discussed above Art 5(1)(c)(2)(ii) mandates the retention of the date and time of the log-in and log-off of the Internet e-mail service. As a single log-in session may last a considerable time the retained data may not be sufficient to establish the point in time an e-mail was sent or received.

[63] For a general discussion of the requirement, see *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Band III, Grundrechte, Art 8 EMRK, § 18.

7.3. "Necessary in a democratic society" for a recognized purpose

Art 8 § 2 ECHR states that an interference must not only be "in accordance with the law" but also be "necessary in a democratic society" for one of the following purposes: national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others.[64]

7.3.1. The public purpose of the Directive

According to Art 1(1) the European legislator aims to harmonize the obligations of providers to retain data, "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime". As Art 8 § 2 ECHR mentions both "national security" and "the prevention of […] crime" this objective can potentially justify the interference with the right to privacy. To determine whether this is actually the case the suitability, necessity and proportionality of the measure have to be examined.

7.3.2. Suitability

Whether the retention of traffic data as provided by the Directive is suitable to achieve the objective stated in Art 1(1) depends on technical aspects of the data retention. It was argued that the amount of data retained would be so vast that a search would take between 50 and 100 years.[65] These estimates are mostly based on incorrect assumptions with regard to what data is to be retained[66] or ignorant of the performance capabilities of today's (high end) computers. When data is indexed[67] dozens of terabytes of data can be searched very efficiently and within adequate time frames.

It has been argued that without the retention of the contents of the communications little information can be gained from the retained data.[68] In addition to that people could use anonymous devices such as a pre-paid cell phone. But as described below traffic analysis

---

[64] See *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht, Band III, Grundrechte, Art 8 EMRK, § 22 et seq.
[65] *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 38.
[66] Westphal seems to assume that HTTP-traffic data is also to be retained; *Westphal*, juridikum 2006, 34, 36.
[67] See *Loney/Theriault*, Oracle9i DBA Handbook (2002), 45 et seq.
[68] *Otto/Seitlinger*, Die „Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, 232.

and social network analysis allows inferring a magnitude of information close to what could be gained from analyzing the contents of a communication.

7.3.3. Necessity

The retention of traffic data can only be considered necessary if it is the least invasive measure available that is suitable to achieve the objective stated in Art 1(1). In this context it is important to reiterate that said objective includes the "detection" of serious crime. This means that measures like the surveillance of a suspect's telecommunications or a "quick freeze" procedure[69] are not a valid alternative as they require that a crime has already been detected or a potential perpetrator of a crime identified.

While it is hard to find a real alternative[70] to the retention of traffic and location data the question arises whether the retention period is as short and therefore as non-intrusive as necessary. According to Art 6 the data is to be retained "for periods of not less than six months and not more than two years". As described above Art 12 additionally allows Member States "facing particular circumstances" to extend the retention period if the Commission and other Member States are informed and the Commission does not reject the extension within six months.

Due to the lack of empirical studies that would clearly demonstrate the extent to which retained data of a certain age is necessary to investigate, detect or prosecute serious crime it is not possible to determine whether two years (or even more) are "necessary".[71] But what can be assumed is that any graph depicting the age of retained data versus the number of crimes for which that data was necessary to investigate, detect or prosecute it would be asymptotic towards 0. This means that there will always be some serious crime that might require a certain kind of data to be retained indefinitely. This clearly shows that the

[69] "Quick freeze" refers to a measure that would allow a national authority to order the retention of a specific person's traffic and location data without having to prove their suspicion. Only when the national authority wants access to the retained data, it has to obtain a court warrant. See *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 38; *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 16; *Article 29 Data Protection Working Party*, Opinion (9.11.2004), 4, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf.

[70] Arguing that traditional investigative measures are equally well suited and therefore constitute a "less intrusive measure", *Otto/Seitlinger*, Die „Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, 233. This argument does not take into account that traffic analysis and social network analysis of the retained data can provide information otherwise unavailable.

[71] *Wüstenberg*, Vorratsdatenspeicherung und Grundrechte, MR-Int 2006, 91, 96.

question of how long the data can be retained under Art 8 § 1 ECHR is rather a question of proportionality than necessity.

7.3.4. Proportionality

The proportionality of this measure particularly depends on its effectiveness, the severity of the interference and the presence of adequate and effective measures against abuse. As the Directive does not regulate the conditions under which national authorities may gain access to the retained data, the public purpose of having such a measure can only be discussed in general terms.

7.3.4.1. Effectiveness with respect to the Directive's objective

The effectiveness of the data retention as provided by the Directive is limited by the inherent limitations of the Directive's scope and the numerous ways to circumvent the retention of one's traffic data in a personally identifiable form.

The Directive's scope is limited in regional terms to the territory of the Member States. This means that providers in third countries have no obligation to retain any data under the Directive. If somebody was to use a dial-up Internet access provided by a third country provider and applies link level encryption then no traffic data could be retained. Another example would be somebody employing end-to-end encryption when communicating with his mail service provider located in a third country. The user's European Internet access provider would be unable to find out to whom e-mails are being sent or from whom they are being received.

A much more drastic limitation of the Directive's scope results from the fact that the categories of data listed in Art 5 are only to be retained with respect to fixed network telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. These means of communication may be the most obvious but by far not the only ones. E-mail and Internet telephony (VoIP) are actually only a very small subset of the means of communication available on today's Internet.

At this point it is important to reiterate that with respect to "Internet access" no data is to be retained "to identify the destination of a communication" (Art 5(1)(b)) or "to identify the type of communication" (Art 5(1)(c)). Internet communication therefore is only to be retained if it is Internet e-mail or Internet telephony.

The Directive does not define either term. As e-mail is a technical term is should also be interpreted in accordance with the relevant technical standards. While RFC 2822[72] specifies the format of an e-mail the RFCs 2821[73], 1939[74] and 3501[75] specify the standard e-mail protocols SMTP, POP3 and IMAP respectively. The term Internet e-mail as used in the Directive has to be construed as data that conforms to RFC 2822 and is being transferred in accordance with RFC 2821, 1939 or 3501. Data transferred over the Internet that does not conform to the aforementioned RFCs is not an "Internet e-mail" and – unless it falls under "Internet telephony" – is not to be retained under Art 5.

As the term "Internet telephony" is not defined in the directive one might recourse to Art 2(2)(c) which defines the term "telephone service" as "calls […], supplementary services […], and messaging and multi-media services (including short message services, enhanced media services and multi-media services)". The term "telephone service" is only used in Art 5(1)(d)(1) to give meaning to the term "type of communication" with respect to fixed network and mobile telephony. The term "telephone service" therefore cannot be used to give meaning to "Internet telephony". If the definition of "telephone service" was applied to the Internet it would effectively cover all services offering audio-visual content. The European legislator hardly wanted to introduce such broad obligations to retain data through a "backdoor", using the term "Internet telephony". The term therefore has to be construed using applicable standards[76] such as SIP (RFC 3261)[77], H.232[78] and RTP (RFC

[72] *Resnick*, RFC 2822, Internet Message Format (2001).
[73] *Klensin*, RFC 2821, Simple Mail Transfer Protocol (2001).
[74] *Myers/Rose*, RFC 1939, Post Office Protocol - Version 3 (1996).
[75] *Crispin*, RFC 3501, Internet Message Access Protocol - Version 4Rev1 (2003).
[76] See *Wallingford*, Switching to VoIP (2005), 119 et seq and 130 et seq.
[77] *Rosenberg/Schulzrinne* et al., RFC 3261, SIP: Session Initiation Protocol (2002).
[78] ITU-T Recommendation H.323, Packet-based multimedia communications systems, http://www.itu.int/rec/T-REC-H.323/en.

3550)[79]. Only data that conforms to these standards can be considered "Internet telephony".

To construe the terms "Internet e-mail" and "Internet telephony" using applicable technical standards is not only a matter of practicality and legal certainty. The whole purpose of the Directive is to obligate providers to retain certain traffic data. To fulfill this obligation providers cannot perform a case-by-case determination of every communication or even every data packet. They have to use automated means to read, analyze, filter and store network traffic data. The implementation of these automated means requires explicit rules as to what data has to be retained. If every provider is not to use his own interpretation of what constitutes "Internet e-mail" or "Internet telephony" they have to use common standards. The aim of the Directive is to harmonize Member States' provisions concerning the obligations of providers with respect to the retention of traffic and location data. As the Directive does not define any technical standards itself, the aim of harmonization can only be fulfilled if already existing generally accepted standards are used. The purpose of the Directive therefore requires that technical terms left undefined in the Directive be construed using technical standards.

As the following means of online communication are neither "Internet e-mail" nor "Internet telephony" they are not to be retained under Art 5: Blogs, message boards, videos on platforms like YouTube, communication via social networking platforms, instant messaging, IRC, Usenet, all HTTP traffic in general and peer-to-peer services.

Blogs (short for "web logs"), message boards or videos on platforms like YouTube may contain a message to one or more individuals but as they are not formatted in accordance with RFC 2822 they cannot be considered an "Internet e-mail". Some forms of communication via social networking platforms may even be labeled "e-mail" by the platform's provider. They nevertheless usually do not adhere to RFC 2822. Instant messaging and IRC allow instant communication between two or more parties. Most instant messaging applications use a proprietary protocol and data format while IRC is

[79] *Schulzrinne/Casner/Frederick/Jacobson*, RFC 3550, RTP: A Transport Protocol for Real-Time Applications (2003).

specified in the RFC 1459[80]. Both can therefore not be considered "Internet e-mail". Usenet uses a message format that is specified in RFC 1036[81]. That format is similar but distinct from RFC 2822. The protocol used to transfer a Usenet message[82] also differs from SMTP. HTTP[83] traffic in general (this includes all communication to and from one's browser) simply is neither "Internet e-mail" nor "Internet telephony". This is even true in the case of web-mail. Web mail service providers like Microsoft, Google or GMX offer their users a website that allows them to authenticate and then send and receive e-mails. Technically speaking the data transferred from the user's browser to the web mail service provier's web server (or vice versa) is not an e-mail (conforming to RFC 2822 being transferred by SMTP, POP3 or IMAP) but an HTTP request or an HTTP response as defined by RFC 2616. When sending an e-mail via web mail data in a proprietary format[84] is transferred to the provider's web server. It is there that the data is formatted in accordance with RFC 2822 and further delivered as an e-mail using SMTP.

It would also be technically infeasible to analyze HTTP-traffic and filter it with respect to web mail. There is no standard that would define how e-mails are to be transferred via HTTP. When looking at received mail using a web mail provider, the provider's web server actually does not send the data comprising the e-mail and the instructions for how to display the data separately. The format language HTML in general does not allow the separation of content and its presentation. This means that any filter that was to attempt to extract relevant e-mail traffic data from the communication with a web mail service provider would have to be changed whenever the design of the web page changes. Given the huge amount of web mail providers and the constant change of their data formats, filtering web mail traffic is impossible for all practical purposes. Due to the imprecision of a filter the inadvertent retention of the content of a communication would also be a statistical necessity.

[80] *Oikarinen/Reed*, RFC 1459, Internet Relay Chat Protocol (1993).
[81] *Horton/Adams*, RFC 1036, Standard for interchange of USENET messages (1987).
[82] *Feather*, RFC 3977, Network News Transfer Protocol (NNTP) (2006).
[83] *Fielding/Gettys* et al., RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1 (1999).
[84] Using custom key-value pairs submitted using the HTTP request method POST; see RFC 2616, Section 9.5.

For all the reasons identified above Art 5 cannot be construed as to obligate providers to analyze and filter any HTTP traffic.[85]

Finally peer-to-peer services are also not covered by the Directive. Due to their decentralized nature they usually are the means of choice for distributing any kind of objectionable content.

As shown above there are many means of online communication for which no data is to be retained under Art 5. This allows people to prevent the retention of their traffic data simply by choosing a different means of communication.

In addition to the inherent limitations of the Directive's scope there are also numerous ways to circumvent the retention of one's traffic data.[86] As previously described one could employ encryption technologies to secure the communication with one's SMTP server. If the recipient of the e-mail also communicates with his mail server always using the encrypted versions of POP3 or IMAP (or uses web mail) the only way an Internet access provider could "see" (i.e. have unencrypted access) to the mail would be the communication between the sender's and the recipient's mail server. While most mail servers transfer e-mails unencrypted, some mail servers do employ encryption by default.[87] In the latter case no retention of traffic data can be performed by Internet access providers.

Another technique to circumvent the retention of one's traffic data would be to use a web mail account as a drop box. If both parties to a communication have the username and password for a certain web mail account they can communicate by saving draft messages in the corresponding "Drafts" folder. As the HTTP traffic with the web mail service does not contain an "Internet e-mail" no traffic data can be retained. As the web mail service provider is not a "provider of publicly available electronic communications services" or of "a public communications network" he is also not obligated to retain any data.

---

[85] Apparently of a different opinion is *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 52.
[86] *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 56.
[87] The carrier grade mail server qmail in certain configurations does exactly that. For example, if the author sends an e-mail using his provider's SMTP server mail.lukasfeiler.com to one of his colleagues at Empowered Media, the receiving mail server mx1.empoweredmail.com will only communicate with mail.lukasfeiler.com using SMTP over TLS. See *Sill*, The qmail Handbook (2002), 264.

There are also circumvention measures that require less technological ingenuity. Public telephone booths usually are not under video surveillance[88]. Another option is the use of a pre-paid cell phone. Most Member States do not require the identification with a government issued ID to purchase such a phone. Even if a Member State did require such an authentication pre-paid cell phones could easily be acquired on the black market. Art 5(1)(e)(2)(vi) makes clear that the European legislator did anticipate this problem. It states that in the case of pre-paid anonymous services the date and time of the initial activation of the service and the cell ID from which the service was activated is to be retained. The idea behind this provision seems to be that people are presumed to buy a pre-paid mobile phone near the place where they live or work. Another simple circumvention measure would be to go to an Internet café or using a public WiFi hot spot.

As further elaborated below, the continuous use of the same "anonymous" communication device (e.g. a pre-paid cell phone) is not a perfect circumvention measure. As soon as the device is used for more than a single conversation, extensive social network analysis might provide clues as to who is using the "anonymous" device. For example, if one uses a pre-paid cell phone to call a friend, a relative and a colleague there might only be one person in the entire population that has direct relations with all three people, and is therefore caller. Pre-paid cell phones nevertheless drastically reduce the effectiveness of the retention of traffic data. Especially drug dealing organizations have been known to use pre-paid cell phones.

With regard to Internet communication there are also more sophisticated circumvention measures. These include commercial anonymization services and onion routing networks. Commercial anonymization services are usually proxy based. Each customer has an encrypted connection with the service provider. Instead of directly communicating with the servers on the Internet users divert all their traffic to the provider's proxy server. The proxy server will then establish a connection with the actual server and forward all traffic between the user and the server. If additional measures are employed to prevent

[88] If a video surveillance was in place it could certainly be defeated by measures like wearing a hat.

information leakage[89], such a commercial service can allow a user to hide his IP address. Another such concept is onion routing. The best known onion routing network is Tor (The Onion Router)[90]. It is a project sponsored by the Electronic Frontier Foundation with an estimated user base of multiple hundred thousand users.[91] Compared to an anonymizing proxy the advantage of onion routing is that a user does not need to trust a single third party. In the Tor network each client randomly selects three proxies (entry, middle and exit node) from a long list of available proxies. Each packet transmitted by the client is encrypted three times. The entry node can only remove the first layer of encryption which will allow it to learn the identity of the middle node. This means that the entry node only knows the identity of the client and the middle node, but not the packet's contents or the identity of the exit node or the server. When the entry node forwards the packet to the middle node, the middle node will be able to remove the second layer of encryption and will therefore learn the identity of the exit node. It however will not know the identity of the client or the server nor will it know the contents of the packet. When the exit node receives the packet from the middle node, it will be able to remove the last layer of encryption and will therefore be the only node that knows the identity of the server. But it does not know the identity of the client (or the entry node). It will know the contents of the packet unless an end-to-end encryption is used between the client and the server (e.g. HTTPS).[92] While Tor also has some weaknesses[93] it certainly constitutes a very strong measure against any retention of traffic data. Even if providers of Tor services were obligated to retain traffic data, Tor servers in third countries could always be used.

The effectiveness of data retention to facilitate the investigation, detection and prosecution of serous crime is therefore severely reduced by both, inherent limitations of the Directive and numerous ways to circumvent the traffic data retention. This necessarily limits the public purpose of this measure itself.

[89] e.g. blocking cookies; see *Kristol/Montulli*, RFC 2109, HTTP State Management Mechanism (1997).
[90] http://tor.eff.org.
[91] https://www.torproject.org/svn/trunk/doc/design-paper/blocking.html.
[92] *Feiler*, Tor als Prüfstein der Data Retention Richtlinie (2005).
[93] See, inter alia, *Bauer/McCoy* et al., Low-Resource Routing Attacks Against Anonymous Systems (2007).

7.3.4.2. Severity of the interference

Now the severity of the interference with the right to privacy has to be examined more closely. The Directive itself does not regulate any uses a national authority might make of the retained data. The possible uses nevertheless do affect the severity of the interference posed by the mere retention of the data. The more information the retained data could potentially reveal about an individual the more severe the interference. The retained traffic and location data does allow for extensive traffic analysis, social network analysis and data mining.

Traffic analysis can use the time and duration of a communication, the identities of the parties communicating, and their location to infer new information.[94] In contrast to cryptanalysis[95] traffic analysis is comparably cheap as less computing power is required. It also does not require a human person to actually look at the analyzed data. As Michael Hermann, the former chair of the UK Joint Intelligence Committee put it: "[it] provides indications of his intentions and states of mind, in rather the same way as a neurologist develops insights about a silent patient by studying EEG traces from the brain"[96].

An almost classic example is a drastic increase of calls placed by Pentagon employees to Domino's Pizza.[97] What can be inferred from this information? Statistically speaking it is a good indicator that hostilities are imminent.[98] Knowing the identity of one party often also reveals at least some content of the communication. If an e-mail is sent to alcoholics-anonymous@example.com the most relevant aspect of the content of the communication can already be inferred with a high probability: the sender is an alcoholic. Similar conclusions can be drawn when a mail is sent to a doctor specialized in cancer treatment or to a criminal defense lawyer. Another example would be that close friends of any individual can usually be identified by determining with whom the individual communicates most often. If multiple calls are initiated by an individual within a short

[94] *Danezis*, Introducing Traffic Analysis - Attacks, Defences and Public Policy Issues (2005), 1.
[95] "The science of recovering the plaintext of a message without access to the key", *Schneider*, Applied Cryptography: Protocols, Algorithms, and Source Code in C² (1996).
[96] *Herman*, Intelligence Power in Peace and War (1996).
[97] *Danezis/Clayton*, Introducing Traffic Analysis (2007), 16.
[98] For an example see *Trausch*, Pizza Politics, Boston Globe, 30.8.1991.

time period the order in which the calls are initiated might indicate a relative importance of the callees to the caller.

Location data might also reveal very interesting facts. If two people that communicate regularly with each other change their location to another part of the country or a different country altogether for a few days, it seems likely that they went on vacation together. If somebody spends the night at a different location (within reach of a different cell) but only regularly communicates with one person in that cell it seems likely that the two people spent the night together.

While traffic analysis would already allow a national authority to infer a lot of information about any individual, social network analysis seems especially well suited for drag net operations and the detection of social structures that might resemble those thought to be typically present in a criminal organization or a terror cell.[99]

Taking things one step further, data mining[100] could be employed to link a database containing retained traffic and location data with other big databases such as those maintained by some national social security agencies.[101]

While all of the above mentioned techniques can be used to investigate and help in the prosecution of serious crimes, they could also be employed to detect these crimes. In this case everybody's communicational behavior would be automatically analyzed for certain "suspicious" communication patterns - irrespective of any anterior suspicion.

The question has been asked whether such a continuous surveillance of the entire population would change the way people behave in private and in public. To what extent would it have a chilling effect on the exercise of the people's fundamental rights. If such or other behavioral modifications do ensue what are the sociological effects? Would social minorities (based on ethnicity, political views, religion or any other factor) feel pressured

[99] *Svenson/Svensson/Tullberg*, Social network analysis and information fusion for anti-terrorism (2006).
[100] Also recognizing the potential of data mining in the context of the Directive, *Westphal*, Die neue EG-Richtlinie zur Vorratsspeicherung, EuZW 2006, 555, 559.
[101] *Bignami*, European versus American liberty: A comparative privacy analysis of antiterrorism data mining (2007).

to assimilate to the main stream so as not raise any suspicions? And haven't most positive sociological developments been started by a social minority – that might now be deterred from voicing their opinion at all? No empirical data is available to answer these questions. They nevertheless raise important issues with respect to the public purpose of deploying such a surveillance measure.

One might argue that techniques like social network analysis and data mining are beyond the capabilities of some Member States. While this may be true, it has to be considered that the European Commission founded numerous security research projects in the PASR ("Preparatory Action in the field of Security Research") program[102]. Among the funded projects is i-TRACS ("Counter-terrorism identification and advanced tracking system using the analysis of communication, financial and travel data")[103] and HiTS-ISAC (Highway to Security/Interoperability for Situation Awareness and Crisis Management)[104]. It is therefore save to assume that the private sector will soon be offering security products and services that do employ social network analysis and data mining.

An issue of special importance (at least from a law enforcement agency's perspective) is that of interoperability between law enforcement agencies in one Member State and data retention databases in another Member State. For this purpose the European Telecommunications Standards Institute (ETSI) is in the process of formulating multiple standards[105] that will clearly define the interfaces a provider has to make available to law enforcement agencies. Technically this will make it possible for a single law enforcement agency to query data retention databases in all other Member States.

---

[102] *Hayes*, Arming Big Brother - The EU's Security Research Programme, TNI Briefing Series 1 (2006).

[103] According the an i-TRACS presentation the project will „ lay the foundations for how data from multiple sources – but with a common thread – can be retrieved, selectively combined in a socio-ethically responsible way, analysed and such intelligence used to optimise the identification of prima facie suspect, or known, terrorists and the tracking of their activities". i-TRACS was funded with € 1,883,826. See http://ec.europa.eu/enterprise/security/doc/project_flyers_2007/I-TRACS.pdf.

[104] According to the document D1.1, "Information requirements of governments and public authorities in combating and protecting against terrorism" (obtainable via e-mail from info@hits-isac.eu) the HITS/ISAC system shall among other things, "supply a tool to generate an intelligence report in daily routine work for each User to analyze the following activities and crisis situation: Bank transaction, Telephone traffic E-Mail traffic, Sensor analysis, Event alert". HITS/ISAC was funded with € 1,209,063. The partners include EADS and the Swedish Defence Research Agency. See http://www.hits-isac.eu/index_files/Page330.htm.

[105] See http://webapp.etsi.org/WorkProgram/Frame_WorkItemList.asp?SearchPage=TRUE&qTITLE=Retained+AND+data&titleType=all.

The research projects and standardization efforts mentioned demonstrate that techniques like traffic analysis and data mining are indeed technically feasible. The retention of traffic and location data that allows for such methods to be deployed constitutes by itself a severe interference with the right to privacy. Adding to the severity of the interference in quantitative terms is the maximum retention period of two years with the possibility of further extensions in accordance with Art 12.[106]

7.3.4.3. Adequate and effective measures against abuse

Another issue to be considered is whether the Directive provides for "adequate and effective measures against abuse". The European Court of Human Rights has repeatedly held[107] that such measures need to be present in order for an interference to be "necessary in a democratic society". In its Art 7 the Council of Europe Convention 108 also mandates "appropriate security measures" to protect the confidentiality, integrity and availability of personal data.

Art 7 of the Directive refers to 95/46/EC and 2002/58/EC and additionally states the following minimum data security principles: (a) the retained data shall be subject to the same security as data on the network; (b) appropriate technical and organizational measures[108] are to be employed to ensure the confidentiality, integrity and availability of the retained data; (c) appropriate technical and organizational measures are to be used to ensure that the retained data can only be accessed by specially authorized personnel[109]; and (d) that data, except those that have been accessed and preserved[110], shall be destroyed at the end of the period of retention. These security measures and the ones to be implemented

[106] See Art 5(e) Council of Europe Convention 108 which explicitly states that personal data shall be "preserved […] for no longer than is required for the purpose for which those data are stored".

[107] E.C.H.R. 6.9.1978, Klass and Others v. Germany, Ser. A no. 28, § 50; see also E.C.H.R. 4.5.2000, Rotaru v. Romania, ECHR 2000-V, § 59 where the term "safeguards" is used instead of „guarantees"; see also *Berka*, Die Grundrechte (1999), § 466.

[108] Information security controls are often defined using the categories administrative (i.e. organizational), physical and technical. Art 7(b) explicitly names organizational and technical controls but does not mention physical controls. See *Landoll*, The Security Risk Assessment Handbook (2006), 35.

[109] This effectively means that the principle of „least privilege" has to be employed. See *Garfinkel/Spafford/ Schwartz*, Practical Unix and Internet Security³ (2003), 235.

[110] This wording raises the question, whether preserved data may never be deleted. See *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 54. Art 7(d) merely exempts said data from a minimum obligation to delete data. National laws implementing 95/46/EC will most likely obligate the provider to delete the data as soon as it is not anymore needed for the purpose it was retained for.

in accordance with 95/46/EC and 2002/58/EC can be considered "adequate and effective" with regard to third parties (everyone except the provider and the national authorities).[111] While administrative security controls should also reduce the risk of misuse by the provider himself[112], insufficient outside review might severely limit the effectiveness of these administrative controls. The supervisory authority provided by Art 9 will most likely effectively not be able to perform an individual security assessment for each provider. In addition to that misuse by national authorities poses a serious risk. At this point it has to be emphasized that the directive 95/46/EC does not apply to law enforcement agencies.[113] Given the ETSI standardization efforts it seems likely that automatic data retrieval will soon be possible for national authorities. Art 10 of the Directive provides that Member States have to submit statistics on a yearly basis to the Commission. Such a measure could deter or allow to detect (but not prevent) misuse by national authorities. But according to Art 14(1) Art 10 is not meant to provide such a measure against abuse.[114] It should rather allow determining whether it is necessary to amend the list of data in Art 5 and the periods of retention provided for in Art 6. As the data protection directives do not regulate security measures to be employed by national authorities the safeguards most likely in place will not be sufficient to reduce the risk of misuse by national authorities to an acceptable level.[115]

7.3.4.4. Conclusion

All of the aforementioned aspects have to be considered and weighed to reach a conclusion as to whether the Directive's interference with the right to privacy is proportional and

[111] A mandatory security breach notification would add to that effectiveness. See COM(2007)698 which proposes to include such an obligation in Art 4(3) 2002/58/EC; http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm.

[112] A more centralized network infrastructure as it is necessitated by the requirement to analyze all traffic creates additional risks of misuse. See *Bellovin/Blaze/Diffie/Landau/Neumann/Rexford*, Risking Communications Security: Potential Hazards of the Protect America Act, IEEE Security & Privacy, January/February 2008 (Vol 6, No 1), 24.

[113] Art 3(2) 95/46/EC explicitly states data processing operations concerning "concerning public security, defence, State security […] and the activities of the State in areas of criminal law" are outside the scope of the directive. See, inter alia, *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 5.

[114] *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 54.

[115] Negating the presence of adequate and effective measures in general (i.e. without regard to the threat agent) *Otto/Seitlinger*, Die „Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227, 232.

"necessary in a democratic society" for the purpose of "national security" or "the prevention of […] crime".

It has been shown above that the traffic and location data retention as provided by the Directive is of limited effectiveness to facilitate the investigation, detection and prosecution of serous crime. If somebody wanted to prevent the retention of his data, there would be numerous ways to achieve that goal. Due to the inherent limitation of the Directive to mobile and fixed network telephony, Internet access, Internet e-mail and Internet telephony, one simply has to choose an alternative means of communication. Internet anonymizing services, pre-paid cell phones, Internet cafés and WiFi hot spots also allow circumventing the retention of traffic and location data in a personally identifiable form. This limited effectiveness reduces the public purpose that has to be weighed against the individual's interest of non-interference with his or her right to privacy.

The possibilities to analyze the retained data in an automatic fashion only slightly add to the effectiveness of the data retention[116] but drastically increase the severity of the interference with the right to privacy. Traffic analysis allows inferring much more information than is apparent from the retained data. This may include sensitive personal information such as medical conditions or sexual orientation. Social network analysis and data mining would especially allow for fishing expeditions[117] and a continuous surveillance of the entire population. People showing social patterns statistically typical for a criminal or terrorist organization, might face more detailed analysis of their data or additional surveillance measures. In addition to the severity of the interference with an individual's right to privacy one could also argue that the potential changes in society resulting from a constant surveillance are contrary to the public purpose.

[116] While possible it can be considered very hard and thereby costly to perform social network analysis and data mining in a way that would allow the identification of a user employing anonymizing technology.
[117] See, inter alia, *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 4.

With a maximum of two years and possibilities of further extension in accordance with Art 12 the retention period also seems excessive by any standard[118] and increases the severity of the interference.

The Directive does not provide adequate and effective measures against abuse by national authorities. Due to a lack of mandatory outside review the measures against abuse by a provider itself are also rather limited.

The public purpose of the data retention is limited by the reduced effectiveness and the potential negative effects on society as a whole. The Directive constitutes a severe interference with the right to privacy and lacks effective measures against abuse. The interference with the right to privacy therefore is not proportionate. The measure is not "necessary in a democratic society" for the purpose of "national security" or "the prevention of […] crime". The Data Retention Directive therefore violates the general Community law principle of the right to privacy.

8. Legality of the Directive with regard to the competences of the EC

It is important to note that the EC (i.e. the first pillar of the EU) does not have any competences with regard to the activities provided for by Title V EU (common foreign and security policy, the second pillar of the EU) and Title VI EU (police and judicial cooperation in criminal matters, the third pillar of the EU). As also expressed in Art 3(2) 95/46/EC personal data processing operations concerning public security, defense, State security and the activities of the State in areas of criminal law fall outside the scope of Community law.[119]

The legal basis for the Directive is Art 95 EC. It states that "[t]he Council shall […] adopt the measures for the approximation of the provisions laid down by law, regulation or

[118] Of a different opinion, arguing that it is „not unthinkable" that a conspiracy begins to take shape and leave communication traces even two years before the crime, *Bignami*, Protecting Privacy against the Police in the European Union: The Data Retention Directive (2007), 18. This argument seems to confuse necessity with proportionality. The latter cannot be satisfied by merely showing that it is not impossible that the interference might advance a public purpose.

[119] See, inter alia, ECJ 20.5.2006, C-318/04, § 54.

administrative action in Member States which have as their object the establishment and functioning of the internal market".

Whether Art 95 EC constitutes an appropriate legal basis for the Directive therefore depends on whether the Directive has as its object "the establishment and functioning of the internal market". Ireland is challenging that assumption and has brought an action for annulment of the Directive under Art 230 EC against the Council of the European Union and the European Parliament.[120]

For Art 95 EC to serve as a legal basis for any measure the measure has to have as its "centre of gravity" the approximation of national laws to benefit the establishment and functioning of the internal market. An incidental effect of harmonizing market conditions is not sufficient.[121]

It is settled case law, that the choice of the legal basis for a measure may not depend simply on an institution' s conviction as to the objective pursued but must be guided by objective factors which are amenable to judicial review, including, in particular, the aim and content of the measure.[122]

8.1. The aim of the Directive

Recital 21 states two objectives for the Directive: "to harmonise the obligations on providers to retain certain data" and "to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime". The wording of Recital 21 seems to suggest an equal weigh of both objectives. Art 1(1) shows a different picture. It states that the Directive "aims to harmonise Member States' provisions concerning the obligations of the providers […] with respect to the retention of certain data […], in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime". The first objective of harmonization is therefore only

[120] C-301/06.
[121] ECJ 17.3.1993, C-155/91, § 19; ECJ 28.6.1994, C-187/93, § 25; ECJ 5.10.2000, C-376/98, § 84.
[122] ECJ 17.3.1993, C-155/91, § 6, Summary § 1; ECJ 28.6.1994, C-187/93, § 17, Summary § 2; ECJ 5.10.2000, C-376/98, § 59; ECJ 4.10.1991, C-70/88, §9, Summary § 1.

pursued “in order to ensure” that the second objective of fighting serious crime can be achieved. Taking Art 1(1) literally, the harmonization is only means to an end.[123]

8.2. The content of the Directive

Under the abovementioned case law the content of a measure has to be examined to determine whether the measure benefits the establishment and functioning of the internal market. To do so, the harmonization with respect to the data to be retained, the providers obligated to retain data, the retention period and the question of reimbursement have to be discussed. Subsequently it will be possible to give an estimate as to the likely effect the Directive will have on the internal market with respect to distortions of competition and barriers to trade.

The obligation to retain data under the Directive is limited to the types of data specified in Art 5(1). The question is whether a Member State could extend that obligation to other types of data. Recital 12 explicitly states that Art 15(1) 2002/58/EC continues to apply to data that does not have to be retained under the Data Retention Directive. Art 15(1) 2002/58/EC under certain conditions allows Member States to adopt legislative measures that restrict the scope of the confidentiality of communications, in particular with respect to traffic data (Art 6 2002/58/EC) and location data (Art 9 2002/58/EC).[124] Art 15(1) 2002/58/EC specifically also allows for Members States to adopt “legislative measures providing for the retention of data for a limited period”.[125] As emphasized by Art 15(1) 2002/58/EC, such measures have to be in conformance with Art 6(1) and (2) EU. This nevertheless means that under Art 15(1) 2002/58/EC, read in conjunction with Recital 12 Member States are allowed to enact laws obligating the retention of other types of data.

Under the Directive only providers of publicly available electronic communications services and providers of public communications networks are obligated to retain data. But

[123] *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 37.
[124] *Wüstenberg*, Die Speicherung von Internetverbindungsdaten nach § 100 TKG im Lichte des EU-Rechts, MR-Int 2007, 136, 137.
[125] ECJ 29.1.008, C-275/06, § 49; *Kosta/Dumortier*, The Data Retention Directive and the principles of European data protection legislation, MR-Int 2007, 130, 131 et seq.; *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34, 35.

under the same conditions as stated in Art 15(1) 2002/58/EC a Member State may very well obligate other providers to retain traffic and location data.[126]

The Directive only provides a minimum of six months and a maximum of two years for the retention period. As discussed above, Art 12 may further allow Member States "facing particular circumstances" to extend the retention period.

The question of reimbursement of the obligated providers is entirely left to the Member States. This will necessarily lead to divergent national rules[127] and therefore to distortions of competition. The problem is further aggravated by the fact that the conditions and the kind of access national authorities may be granted by different Member States will result in varying costs providers will have to face in each Member State.

What the Directive effectively does is to provide a minimum with regard to most aspects of the retention of traffic and location data. Due to the fact that the perception of what is needed in the fight against terrorism and other serious crimes differs greatly among the Member States the provided minimum will not lead to harmonized national rules.[128] The resulting diverging data retention obligations will continue to constitute trade barriers. The Directive's effect on the internal market will ultimately be a negative one. Creating new data retention obligations without providing for harmonized reimbursements will very likely create new distortions of competition.[129]

8.3. A comparison with C-317/04 (passenger name records)

In its judgment in the case C-317/04[130] the ECJ nullified the Council Decision 2004/496/EC on the conclusion of an Agreement between the EC and the U.S. on the processing and transfer of PNR data by Air Carriers to the U.S. Department of Homeland

[126] See, inter alia, § 113a(3) of the German Telekommunikationsgesetz which mandates that mail service providers also retain data.
[127] See, inter alia, *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 50; *Westphal*, Die neue EG-Richtlinie zur Vorratsspeicherung, EuZW 2006, 555, 557.
[128] *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49, 50.
[129] See also *Gitter/Schnabel*, Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411, 412.
[130] ECJ 20.5.2006, C-317/04; see *Simitis*, Übermittlung von Flugpassagierdaten, NJW 2006, 2001.

Security. The agreement stated that the transferred data was to be used to combat terrorism and other serious crime.

The Council of the European Union, which was the defendant in the case, argued that the Decision intended to eliminate any distortion of competition, between the Member States' airlines and between the latter and the airlines of third countries, which could result from the requirements imposed by the United States.[131] The critical argument was that the initial processing of the data was carried out by the airlines for commercial purposes. The subsequent transmission for the purpose of combating terrorism and other serious crimes should therefore not be seen as outside of the competence of the EC.[132] But the Court decided to treat the two acts of initial processing and subsequent transmission separately. As the transmission itself occurs for the purpose of combating terrorism and other serious crimes, the EC was found not to have a competence under Art 95 EC to regulate the issue.

In C-317/04 the two acts consisted of the collection (including initial processing) and the transmission of the data. In the context of the Data Retention Directive the first act usually is the processing of data to the extent that is necessary to convey data signals on the communication network. The second act is the retention of the data. As it was the case in C-317/04, the first act is carried out for commercial purposes, while the second act seems to serve at least primarily the purpose of combating serious crimes.

8.4. Conclusion

Art 95 EC may only serve as a legal basis for the Directive if it has as its object "the establishment and functioning of the internal market". As shown above, the aim and the content of the directive clearly indicate that the "centre of gravity" of the measure is the "investigation, detection and prosecution of serious crime" and not the "establishment and functioning of the internal market". Due to the lack of harmonized reimbursements it even seems likely that the Directive will effectively create new distortions of competition.

[131] ECJ 30.5.2006, C-317/04, § 64; the United States authorities refused to waive the right to impose penalties on airlines failing to comply with U.S. legislation that mandated electronic access to PNR data. See ECJ 30.5.2006, C-317/04, § 33.
[132] ECJ 30.5.2006, C-317/04, § 66.

On the merits, it therefore seems likely that the Court will nullify the Data Retention Directive in the pending case C-301/06 due to a lack of competence under Art 95 EC.

Bibliography

All URLs are valid as of April 25, 2008.

Analysys, Final Report for the European Commission: IP Voice and Associated Convergent Services (2004), http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/studies_ext_consult/ip_voice/401_28_ip_voice_and_associated_convergent_services.pdf

Bauer/McCoy et al., Low-Resource Routing Attacks Against Anonymous Systems (2007), http://www.cs.colorado.edu/department/publications/reports/docs/CU-CS-1025-07.pdf

Bellovin/Blaze/Diffie/Landau/Neumann/Rexford, Risking Communications Security: Potential Hazards of the Protect America Act, IEEE Security & Privacy, January/February 2008 (Vol 6, No 1)

Benn-Ibler, Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten, AnwBl 2008, 12

Berka, Die Grundrechte (1999)

Bignami, European versus American liberty: A comparative privacy analysis of antiterrorism data mining, 48 Boston College Law Review 609 (2007), http://eprints.law.duke.edu/1603/1/48_B.C.__L._Rev_609_(2007).pdf

Bignami, Protecting Privacy against the Police in the European Union: The Data Retention Directive, Mélanges en l'Honneur de Philippe Léger: Le Droit à la Mesure de l'Homme (2006), http://ssrn.com/abstract=955261

Crispin, RFC 3501, Internet Message Access Protocol - Version 4Rev1 (2003)

Danezis, Introducing Traffic Analysis - Attacks, Defences and Public Policy Issues (2005), http://homes.esat.kuleuven.be/~gdanezis/TAIntro.pdf

Danezis/Clayton, Introducing Traffic Analysis (2007), 16, http://homes.esat.kuleuven.be/~gdanezis/TAIntro-book.pdf.

Feather, RFC 3977, Network News Transfer Protocol (NNTP) (2006)

Feiler, Tor als Prüfstein der Data Retention Richtlinie (2005), http://www.lukasfeiler.com/Tor.pdf

Fielding/Gettys et al., RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1 (1999)

Fowein/Peukert, Europäische Menschenrechtskonvention² (1996)

Landoll, The Security Risk Assessment Handbook (2006)

Garfinkel/Spafford/Schwartz, Practical Unix and Internet Security³ (2003)

Gitter/Schnabel, Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411

Gschweitl/Langmantel/Reichinger, Voice over IP - Rechtliche Einordnung eines neuen Konzeptes, MR 2005, 503

Harris, CISSP All-in-One Exam Guide³ (2005)

Hayes, Arming Big Brother - The EU's Security Research Programme, TNI Briefing Series 1 (2006), http://www.tni.org/reports/militarism/bigbrother.pdf

Herman, Intelligence Power in Peace and War (1996)

Horton/Adams, RFC 1036, Standard for interchange of USENET messages (1987)

International Telecommunication Union, ITU-T Recommendation E.212, The international identification plan for mobile terminals and mobile users, http://www.itu.int/rec/T-REC-E.212-200405-I/en.

International Telecommunication Union, ITU-T Recommendation H.323, Packet-based multimedia communications systems, http://www.itu.int/rec/T-REC-H.323/en.

Klensin, RFC 2821, Simple Mail Transfer Protocol (2001)

Korinek/Holoubek, Österreichisches Bundesverfassungsrecht, Band III, Grundrechte

Kosta/Dumortier, The Data Retention Directive and the principles of European data protection legislation, MR-Int 2007, 130

Kristol/Montulli, RFC 2109, HTTP State Management Mechanism (1997)

Liebwald, The New Data Retention Directive, MR-Int 2006, 49

Loney/Theriault, Oracle9i DBA Handbook (2002)

Myers/Rose, RFC 1939, Post Office Protocol - Version 3 (1996)

Oikarinen/Reed, RFC 1459, Internet Relay Chat Protocol (1993)

Otto/Seitlinger, Die „Spitzelrichtlinie“: Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227

Resnick, RFC 2822, Internet Message Format (2001)

Schulzrinne/Casner/Frederick/Jacobson, RFC 3550, RTP: A Transport Protocol for Real-Time Applications (2003)

Schneider, Applied Cryptography: Protocols, Algorithms, and Source Code in C² (1996)

Sill, The qmail Handbook (2002)

Simitis, Übermittlung von Flugpassagierdaten, NJW 2006, 2001

Stevens, TCP/IP Illustrated, Volume 1 (1994)

Svenson/Svensson/Tullberg, Social network analysis and information fusion for anti-terrorism (2006), http://www.foi.se/infofusion/bilder/CIMI_2006_S3_1.pdf.

Trausch, Pizza Politics, Boston Globe, 8/30/91, http://home.xnet.com/~warinner/pizzacites.html#bo_globe

Rosenberg/Schulzrinne et al., RFC 3261, SIP: Session Initiation Protocol (2002)

Wallingford, Switching to VoIP (2005)

Warner, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, University of Ottawa Law & Technology Journal, Vol. 2, No. 1 (2005), 75, http://ssrn.com/abstract=777844

Westphal, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, juridikum 2006, 34

Westphal, Die neue EG-Richtlinie zur Vorratsspeicherung, EuZW 2006, 555

Wüstenberg, Die Speicherung von Internetverbindungsdaten nach § 100 TKG im Lichte des EU-Rechts, MR-Int 2007, 136

Wüstenberg, Vorratsdatenspeicherung und Grundrechte, MR-Int 2006, 91

Abbreviations

Art	Article
e.g.	exempli gratia
et seq.	et sequentes or et sequential
i.e.	id est
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
E.C.H.R.	European Court of Human Rights
ECJ	European Court of Justice
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
POP3	Post Office Protocol, Version 3
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP