EJLT European Journal of Law and Technology

The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection

Lukas Feiler [1]

Cite as: Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", European Journal of Law and Technology, Vol. 1, Issue 3, 2010.

Abstract:

The EU Data Retention Directive (2006/24/EC) provides an obligation for providers of publicly available electronic communications services and 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 fundamental rights to privacy and data protection as guaranteed by the Charter of Fundamental Rights of the European Union.

1. Introduction

The Data Retention Directive [2] (hereinafter *the Directive*) provides an obligation for providers of publicly available electronic communications services and for providers 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. This marks a departure from EU data protection principles under Directive 95/46 [3] (hereinafter *Data Protection Directive*) and Directive 2002/58 [4] (hereinafter *ePrivacy Directive*).

After the acts of terrorism committed in 2001 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 to protect security. [5] The Directive certainly fits the bill. It was officially proposed by the Commission in September 2005 [6] after the European Council had expressed an interest in such a measure following the Madrid terrorist bombings, [7] and had emphasized its priority following the London terrorist bombings. [8]

The first legal challenge to the Directive was a formalistic one. In *Ireland v. Council and Parliament*, [9] Ireland asked the European Court of Justice (ECJ) to annul the Directive on the grounds that it was not adopted on an appropriate legal basis. The Directive had been adopted pursuant to European Community (EC) Treaty [10] article 95 (now TFEU [11] article 114), which requires a legal act to have as its 'centre of gravity' the approximation of national laws to benefit the functioning of the internal market. [12] Ireland contended that the main or predominant purpose of the Directive was, however, to facilitate the investigation, detection, and prosecution of serious crime, including terrorism. A legal act with such a purpose, Ireland argued, could only have been adopted under EU Treaty [13] Title VI ('police and judicial cooperation in criminal matters'). The ECJ declined to follow, upholding the Directive. [14] The Court held that the substantive content of the Directive 'is directed essentially at the activities of service providers in the relevant sector of the internal market' [15] and that '[t]hose matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the [Directive].' [16]

While the ECJ has authoritatively answered the question of whether the legal basis is appropriate, the Court has not yet addressed another - and arguably more important- issue: whether the Directive violates EU fundamental rights, in particular the fundamental right to privacy and the fundamental right to data protection as guaranteed by article 7 and article 8 of the Charter of Fundamental Rights of the European Union [17] (hereinafter *Charter*) which entered into force with the adoption of the Lisbon Treaty [18] on December 1, 2009. [19]

This article's contribution is twofold: First, it will provide a technically founded analysis of the scope of the Directive. In the few instances when such a technical analysis was provided by prior research, it was exclusively focused on Internet-related traffic data. [20] Second, the article will provide an assessment of the legality of the Directive in light of the Charter.

The following chapters 2 to 6 will first analyze the substance of the Directive. Chapter 7 will then discuss whether the Directive meets the requirements under article 7 and article 8 of the Charter.

2. The Personal Scope of the Obligation to Retain Data

Article 3 states that only 'providers of publicly available electronic communications services' and providers of 'public communications networks' are obligated to retain any data. Article 2(1) refers to the definitions provided by Parliament and Council Directive 2002/21 (hereinafter *Framework Directive*). [21]

Framework Directive article 2(c) 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.' Framework Directive article 2(c) requires that the service wholly or mainly consist 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 Model [22]: the physical layer, the data link layer, and the network layer. [23]

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 layer, and the transport layer. [24] They do not concern themselves with the first three layers of the OSI Model, i.e. with the 'conveyance of signals.'

Recital 10 of the Framework Directive seems to contradict Framework Directive article 2(c) when it states that '[v]oice telephony and electronic mail conveyance services are covered by this Directive.' However, the term 'conveyance,' as it is used in recital 10 of the Framework Directive, is to be understood in the same context as it is used in Framework Directive article 2(c). The person conveying an email 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 that 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 article 3 of the Directive.

A similar question is raised with regard to providers of Internet telephony services. [25] Here it is necessary to differentiate between a Voice over Internet Protocol (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. [26] 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 article 3 of the Directive.

The second kind of providers named in article 3 are providers of 'public communications networks.' Framework Directive article 2(d) defines the term 'public communications network' as 'an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services.' Framework Directive article 2(a) 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 article 3 therefore is the entity that provides the network infrastructure that permits the conveyance of signals.

3. Transposition of the Directive

Pursuant to article 15(1), Member States had to transpose the Directive by September 15, 2007. According to article 15(3), Member States had the option of postponing the Directive's transposition until March 15, 2009 but only with regard to Internet access, Internet e-mail, and Internet telephony. [27] Sixteen Member States chose to do so.

Indicative of the controversial nature of the Directive, many Member States faced domestic obstacles in the process of transposing the Directive into national law. The European Commission chose to bring infringement actions against Greece, [28] the Netherlands, [29] Sweden, [30] and Austria. [31] Sweden, despite having lost its case before the ECJ, still refuses to transpose the Directive, citing human rights concerns. [32] In the case against Austria, which was the only Member State to formally raise the issue of whether the Directive conforms to fundamental rights, the ECJ held that a Member State cannot properly plead the unlawfulness of a directive as a defence in an infringement action under TFEU article 258. [33]

Documents released by the European Commission in response to a request for access to documents under Charter article 42 reveal that the Commission has also initiated infringement proceedings against Luxembourg. [34]

In Germany and Romania where the Directive had been transposed, constitutional courts struck down the transposing acts as violating constitutional rights. The Constitutional Court of Romania held that the transposing act violated the constitutional rights of privacy, of confidentiality in communications, and of free speech. [35] The German Federal Constitutional Court - without addressing the legality of the Directive itself [36] - declared the transposing act unconstitutional as it violated the privacy of telecommunications guaranteed by Basic Law [37] article 10(1). [38] The Federal Constitutional Court held that, while the scope of data to be retained was not per se disproportional, the statutory requirements regarding data security, the purposes of data processing, transparency, and legal protection were insufficient, [39] rendering the transposing legislation disproportional. Over 34,000 citizens, including Sabine Leutheusser-Schnarrenberger, currently serving as Germany's Federal Minister of Justice, had initiated this action.

4. Data to Be Retained

4.1. General Limitations

Article 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.' [40] As article 2(1) refers to the Data Protection Directive with regard to the definitions contained therein, the term 'processed' has to be construed according to Data Protection Directive article 2(b) 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.

Recital 13 explicitly states that only 'accessible' data has to be retained. It further notes with regard to Internet e-mail and Internet telephony that the obligation to retain data applies 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 as referring to a 'publicly available electronic communications service.' [41]

A further limitation is provided by article 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. [42] A simple example would be regular calls to a cardiologist only occurring during office hours. Article 5(2) therefore seems to essentially contradict article 5(1). To resolve this contradiction one has to interpret the phrase 'data revealing the content' in article 5(2) as data 'containing' or 'directly revealing' the content. This can also be supported by the last sentence of article 1(2) which states that '[the Directive] shall not apply to the content of electronic communications.' This means that article 5(2) only emphasizes what is obvious from article 5(1): the content of communications must not be retained pursuant to the Directive. [43]

4.2. Traffic Data Categories and Affected Means of Communication

Article 5(1) names six categories of data to be retained: data necessary to (a) trace and identify the source of a communication; (b) identify the destination of a communication; (c) identify the date, time, and duration of a communication; (d) identify the type of communication; (e) identify users' communication equipment or what purports to be their equipment; and (f) identify the location of mobile communication equipment. While this list of data categories is very broad, the means of communication to which they apply are rather few, significantly reducing the scope of data to be retained.

According to article 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. [44]

When fixed network telephony or mobile telephony is used for communication, the telephone number, name, and address [45] of the caller and the callee(s), the date and time of the start and end of the communication, [46] and the type of telephone service used [47] are to be retained. For mobile telephony the caller and the callee(s) International Mobile Subscriber Identity (IMSI), [48] International Mobile Equipment Identity (IMEI), [49] and cell ID [50] 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 are also to be retained. The data relating to unsuccessful call attempts does not have to be retained. [51]

With regard to Internet access, the following data has to be retained: the allocated IP address, [52] user ID(s), [53] the calling telephone number in case of dial-up access, [54]

the name and address of the person to whom the IP address was allocated, [55] the date and time of the log-in and log-off, [56] and the DSL or other end point (on the user's side). [57] 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' (article 5(1)(b)) or 'to identify the type of communication' (article 5(1)(d)). [58] With regard to Internet e-mail and Internet telephony, 'Internet access' therefore is not a subsidiary 'catch-all' means of communication.

Regarding Internet e-mail, the sender's and the recipient's e-mail addresses (hereinafter *user IDs*), [59] telephone numbers in case of dial-up access, [60] DSL or other end points (on the user's side), [61] names, and addresses [62] are to be retained. To identify the date, time, and duration of the communication, article 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. However, as the wording of article 5(1)(c)(2)(ii) makes clear, the log-in and log-off time of the Internet e-mail service has to be retained, but not the point in time an e-mail was actually sent or received. The Directive does not define the term 'Internet e-mail service.' The term certainly covers services offered using the standardized e-mail protocols SMTP, [63] POP3, [64] and IMAP. [65]

To identify the type of e-mail communication, information about 'the Internet service used' has to be retained. [66] However, the Directive does not provide a definition for the term 'Internet service.' Article 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 e-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 ('user IDs'), [67] names, and addresses; [68] in case of a VoIP-to-telephone-network-call, the callee's telephone number and the telephone number assigned to the caller, [69] telephone numbers in case of dial-up Internet access, [70] DSL or other end points (on either user's side), [71] the date and time of the log-in and log-off of the Internet telephony service, [72] and the type of Internet service used. [73] '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 identifying the geographic location of the cell) has to be retained at the start of the communication. [74]

5. The Minimum and Maximum Retention Periods

Article 6 states that the data specified in article 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.' This gives the Member States considerable flexibility in determining the retention period. Adding to this flexibility is article 12, [75] which 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 article 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 article 5. The Directive therefore does not establish a general maximum data retention period.

6. Access to Retained Data

Article 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 European Community had no power to regulate the issue of access by national authorities for activities referred to in the first indent of Data Protection Directive article 3(2). These include 'processing operations concerning public security, defence, State security […] and the activities of the State in areas of criminal law.' [76]

When interpreting article 4 in the light of recital 25, it is apparent that the Directive sets no limits whatsoever on the conditions or kind of access to the retained data a Member State may grant a national authority. [77] Article 1 also 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*' [78] (emphasis added).

7. Legality of the Directive with Regard to Fundamental Rights

When determining the legality of the Directive with regard to 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. However, as further elaborated *infra*, the Directive does provide that the purpose of the data retention is 'the investigation, detection and prosecution of serious crime.' [79]

7.1. Interference with the Rights to Privacy and Personal Data Protection

Before the adoption of the Lisbon Treaty, EU Treaty article 6(2) was the sole legal basis for fundamental rights in EU law. It stated that the EU 'shall respect fundamental rights […]

as general principles of Community law.' Pursuant to EU Treaty article 6(2), said fundamental rights were to be derived from the Convention for the Protection of Human Rights and Fundamental Freedoms [80] (hereinafter *ECHR*) and from the constitutional traditions common to the Member States. [81]

With the adoption of the Lisbon Treaty on December 1, 2009, the Charter entered into force. EU Treaty 6(1) as amended by the Lisbon Treaty states that '[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union [...] which *shall have the same legal value as the Treaties*' (emphasis added). The Charter is therefore part of primary EU law and all acts of secondary EU law - in particular directives - have to conform to it. [82] Accordingly, it is possible to challenge the legality of the Directive on the basis that it does not conform with the Charter. [83]

Article 7 of the Charter ('Respect for private and family life') states: 'Everyone has the right to respect for his or her private and family life, home and communications.'

Article 8(1) of the Charter ('Protection of personal data') provides: 'Everyone has the right to the protection of personal data concerning him or her.'

The preamble of the Charter provides guidance for interpreting its provisions. It states:

> This Charter reaffirms [...] the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, [...] the European Convention for the Protection of Human Rights and Fundamental Freedoms, [...] and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights.

Specifically regarding the rights which correspond to rights guaranteed by the ECHR, article 52(3) of the Charter states that 'the meaning and scope of those rights shall be the same as those laid down by the [ECHR].' It is important to note that the ECHR only constitutes a floor not a ceiling for the level of protection provided by the Charter. [84]

The case law of the European Court of Human Rights is particularly relevant as it addresses many questions related to communications surveillance and data privacy. Furthermore, both article 7 and article 8 of the Charter are based on ECHR article 8. [85]

ECHR article 8 § 1 stipulates everybody's right 'to respect for his private and family life, his home and his correspondence.' [86] The European Court of Human Rights established in *Klass v. Germany* [87] that telephone communications fall under both 'correspondence' and 'private life.' [88] The Court has further held in *Malone v. United Kingdom* [89] that not just the contents of telephone communications but also the telephone numbers dialled (i.e. traffic data) are protected under ECHR article 8. In *Copland v. United Kingdom*, [90] the court held that this principle also applies to e-mail communication.

Article 7 of the Charter uses the same wording as article 8 ECHR, except that the broader term 'communications' instead of 'correspondence' is used. [91] In light of the above case law, it is evident that the means of communication addressed by the Directive-fixed network telephony, mobile telephony, Internet access, Internet e-mail, and Internet telephony-fall within the scope of article 7 of the Charter.

As the Directive does not regulate the conditions under which access to the retained data

may be granted, the issue arises whether the data retention in itself constitutes an interference with article 7 and article 8 of the Charter. The European Court of Human Rights stated in *Amann v. Switzerland* that 'the storing of data relating to the 'private life' of an individual falls within the application of Article 8 § 1 [ECHR].' [92] Citing this principle, the Court further elaborated in *Copland v. United Kingdom* that 'it is irrelevant that the data held [...] were not disclosed or used [...] in disciplinary or other proceedings.' [93] The right to privacy as it is provided by ECHR article 8 is therefore to be understood in a very broad sense.

As the scope of article 7 and article 8 of the Charter has to be construed as at least equally broad, [94] the retention of traffic data in itself constitutes an interference with article 7 and article 8 of the Charter. 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 these rights. The question therefore is whether this interference constitutes a violation.

With regard to potential limitations of the rights guaranteed by the Charter, article 52(1) of the Charter provides:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

This is very similar to the requirements established by ECHR article 8 § 2 which states that an interference with the exercise of the right conferred by article 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. 'Provided for by Law'

The European Court of Human Rights has repeatedly held that the phrase 'in accordance with the law' in ECHR article 8 § 2 also establishes requirements with regard to the quality of the law and does not only refer back to domestic law. [95] Said quality has to be compatible with the rule of law, which is expressly mentioned in the preamble to the ECHR. To that end, it has to fulfil the requirement of foreseeability, [96] i.e. it has to be 'formulated with sufficient precision to enable any individual - if need be with appropriate advice - to regulate his conduct.' [97] The Charter's requirement that any limitation on the exercise of rights 'must be provided for by law' is to be construed to establish the same requirements. [98]

Article 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, article 5 is also ignorant of certain technical facts [99] and thereby specifies the data to be retained less precisely than intended.

However, with sufficient technical understanding of the communication technologies involved, all terms used in article 5 can be applied to the five types of communication in a way that foreseeability can be established with respect to what data will be retained.

7.3. The Requirements of the Principle of Proportionality

Article 52(1) of the Charter refers to the 'principle of proportionality.' It is established case law of the ECJ that

> [t]he principle of proportionality, which is one of the general principles of Community law, requires that measures adopted by Community institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued. [100]

From the ECJ's case-law and article 52(1), four elements of the proportionality test can be inferred. For an interference with a fundamental right to be proportionate, the measure must: (1) pursue 'objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;' [101] (2) be suitable to meet these objectives; (3) be 'necessary' in the sense that it is the least invasive suitable measure; and (4) is proportionate in the strict sense. [102] Each of these elements will be discussed below.

Note that ECJ's measure of proportionality slightly differs from that used by the European Court of Human Rights. [103] However, since the ECJ and not the European Court of Human Rights will have to rule on whether the Directive complies with the Charter, the ECJ's measure is used in this article. [104]

7.3.1. The Public Purpose of the Directive

Under the principle of proportionality, a measure that interferes with a fundamental right can only be justified if it pursues a legitimate public purpose. The fundamental right to the protection of personal data under Charter article 8 also requires that personal data be only processed for specified and legitimate purposes. [105]

According to article 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 TFEU [106] article 82 et seq. grant upon the EU powers in the area of judicial cooperation in criminal matters, the 'investigation, detection and prosecution of serious crime' evidently is a 'general interest recognised by the Union' [107] as required by the principle of proportionality. Furthermore, the Directive's stated purpose, despite being worded very broadly, [108] also fulfils the requirement of a specified and legitimate purpose under Charter article 8.

The Directive's objective has the potential to justify an interference with article 7 and

article 8 of the Charter. To determine whether this is actually the case, the suitability, necessity, and proportionality *stricto sensu* 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 article 1(1) depends on the technical aspects of the data retention. Commentators have argued that the amount of data retained would be so vast that a search would take between 50 and 100 years. [109] These estimates are mostly based on incorrect assumptions with regard to what data is to be retained [110] and ignorant of the performance capabilities of today's computer systems. When properly indexed, [111] large amounts of retained data can be searched very efficiently and within adequate time frames.

It has also been argued that without the retention of the contents of the communications, little information can be gained from the retained data. [112] However, as described below, traffic analysis and social network analysis allow inferring a magnitude of information, close to what could be gained from analysing the contents of communications.

Furthermore, one might argue that the Directive cannot achieve its objective due to the numerous ways to circumvent the retention of one's traffic data. [113] This argument, however, fails because the suitability test only requires that the measure is not 'manifestly' unsuitable. [114]

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 article 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 specific suspect's telecommunications or a 'quick freeze' procedure [115] are not a suitable alternative as they require that a crime has already been detected or a potential perpetrator of a crime identified. [116]

While it is hard to find a real alternative [117] to the retention of traffic and location data, the question arises whether the retention period is as short and therefore only as non-intrusive as necessary. According to article 6, the data is to be retained 'for periods of not less than six months and not more than two years.' As described above, article 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 object to the extension within six months.

Due to the lack of empirical studies [118] that would 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.' [119] What can be assumed, however, 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 zero. 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 question of how long the data can be retained while not violating article 7 and article 8 of the Charter is rather a question of proportionality *stricto sensu* than necessity.

7.3.4. Proportionality *Stricto Sensu*

The proportionality of the Directive particularly depends on three factors: 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.

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 available to circumvent the retention of one's traffic data in a personally identifiable form.

The Directive's scope is limited in geographic terms to the territory of the Member States. This means that providers in third countries naturally 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, [120] no traffic data could be retained. Another example would be somebody employing end-to-end encryption when communicating with his mail service provider. [121] The user's Internet access provider in the EU 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 article 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 have been the most obvious ones at the time the Directive was drafted. However, 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' (article 5(1)(b)) or 'to identify the type of communication' (article 5(1)(c)). Internet communication therefore is only to be retained if it is Internet e-mail or Internet telephony.

The Directive defines neither the term 'Internet e-mail' nor 'Internet telephony.' As the term 'e-mail' is of a technical nature, it should be interpreted in accordance with the relevant technical standards. While Request for Comments [122] (RFC) 5322 [123] specifies the format of an e-mail, the RFCs 5321, [124] 1939, [125] and 3501 [126] 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 5322 and is being transferred in accordance with RFC 5321, 1939, or 3501. Data transferred over the Internet that does not conform to the aforementioned RFCs is not 'Internet e-mail.' Related traffic data is therefore not to be retained under article 5.

As the term 'Internet telephony' is not defined in the Directive, one might take recourse to article 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 article 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 'Internet telephony' therefore has to be construed using applicable standards [127] such as SIP (RFC 3261), [128] H.232, [129] and RTP (RFC 3550). [130] 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 fulfil 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 goal of harmonisation 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 article 5: blogs, message boards, video platforms (e.g. YouTube), social networking platforms (e.g. Facebook), [131] instant messaging, Internet Relay Chat (IRC), Usenet, all Hypertext Transfer Protocol (HTTP) traffic in general, and peer-to-peer services.

Blogs (short for 'web logs'), social networking or video platforms may contain a message to one or more individuals but as they are not formatted in accordance with RFC 5322, they cannot be considered 'Internet e-mail.' Some forms of communication via social networking platforms may even be labelled 'e-mail' by the platform's provider. They nevertheless typically do not adhere to RFC 5322. 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 specified in the RFC 1459. [132] Both can therefore not be considered 'Internet e-mail.' Usenet uses a message format that is specified in RFC 5536. [133] That format is similar but distinct from RFC 5322. The protocol used to transfer a Usenet message [134] also differs from SMTP. HTTP [135] traffic (this generally includes all communication to and from one's web browser) 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 provider's web server (or vice versa) is not an e-mail (conforming to RFC 5322 being transferred by SMTP, POP3, or IMAP) but an HTTP request or an HTTP response as defined in RFC 2616. When sending an e-mail via web-mail, data is transferred to the provider's web server in a proprietary format. [136] It is there that the data is formatted in accordance with RFC 5322 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 provide for 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 number 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 occur with statistical necessity. For all the reasons identified above, article 5 cannot be construed as to obligate providers to analyze and filter any HTTP traffic. [137]

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 article 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. [138] 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 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. [139] 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 provider 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' it is also not obligated to retain any data.

Furthermore, there are circumvention measures that require less technological ingenuity for concealing one's identity. These include the use of public telephone booths and pre-paid cell phones. Most Member States do not require that the buyer of a pre-paid cell phone identify herself with a government-issued photo ID. Even if a Member State did require such an authentication, pre-paid cell phones could easily be acquired on the black market. Article 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. Acting contrary to that assumption constitutes another circumvention measure. Regarding Internet access, a simple circumvention measure would be to go to an Internet café or to use 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, making it feasible to identify the caller. Pre-paid cell phones nevertheless drastically reduce the effectiveness of the retention of traffic data. [140]

With regard to Internet communication, there are also more sophisticated circumvention measures. These include commercial anonymisation services and onion routing networks. Commercial anonymisation 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 information leakage, [141] such a commercial service can allow a user to hide her IP address and thereby her identity.

Another such concept is onion routing. The best known onion routing network is Tor (The Onion Router). [142] It is a project sponsored by the Electronic Frontier Foundation with an estimated user base of multiple hundred thousand users. [143] Compared to an anonymising 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 (referred to as 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. However, 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 [144]). [145] While Tor also has some weaknesses, [146] it does constitute 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 to circumvent such obligations.

The effectiveness the Directive with regard to facilitating the investigation, detection. and prosecution of serious 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 measure's public purpose.

Severity of the Interference

At this point, the severity of the interference with article 7 and article 8 of the Charter has to be examined more closely. First, it has to be emphasized that the Directive is a blanket measure in the sense that it mandates the retention of personal data irrespective of who it relates to. This factor weighs heavily against the proportionality of the Directive: In *S. and Marper v. United Kingdom*, the European Court of Human Rights stated that it was 'struck by the blanket and indiscriminate nature' of UK laws that allowed fingerprints, cellular samples, and DNA profiles to be retained for all individuals suspected of a criminal offence but 'irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender.' [147]

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. [148] In contrast to cryptanalysis, [149] traffic analysis is relatively inexpensive, because 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: 'traffic analysis […] 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.' [150]

An almost classic example is a drastic increase of calls placed by Pentagon employees to Domino's Pizza. [151] What can be inferred from this information? Statistically speaking, it is a good indicator that hostilities are imminent. [152] Knowing the identity of one party often also reveals at least some contents 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 defence 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 time period, the order in which the calls are initiated might also indicate a relative importance of the callees to the caller. [153]

Location data might also reveal very significant facts. If two people who 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. [154]

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 organisation or a terror cell. [155]

Taking things one step further, data mining [156] 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. [157]

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

Any effort to 'detect' very rare but vaguely defined behaviour within an entire population -like 'terroristic activities' - raises particularly grave concerns. This is due to the characteristic of 'false positive' and 'false negative' error rates when dealing with a 'needle in a haystack' problem. In this context, a 'false positive' signifies an individual who is incorrectly identified as a 'terrorist.' A 'false negative' signifies a terrorist incorrectly identified as 'not a terrorist.' Let us assume that there are one hundred 'terrorists' within the EU population of 500 million, [158] and the existence of a data mining program that has a 1 in 100 false positive rate and a 1 in 100 false negative rate (99 percent accuracy). What is the probability that a person identified by the system as a terrorist actually is one? It is not 99 percent as one might intuitively assume, [159] but rather about 0,002 percent (or 1 in 50,000). The system will incorrectly identify about 5 million people as terrorists while correctly identifying 99 terrorists. [160] While 1 to 50,000 seems disproportionate enough, it should be noted that the assumption that it is possible to construct a 'profile' as precise as matching 99 percent of all terrorists but only 1 percent of the rest of the population is, at best, very optimistic. [161]

One might question whether Member States have the capabilities to engage in such 'drag net' operations. In this regard, it has to be emphasized that the European Commission funded numerous relevant security research projects in the PASR ('Preparatory Action in the field of Security Research') program. [162] Among the funded projects was i-TRACS ('Counter-terrorism identification and advanced tracking system using the analysis of communication, financial and travel data') [163] and HiTS-ISAC (Highway to Security/Interoperability for Situation Awareness and Crisis Management). [164] As demonstrated by products and services developed by the private sector, this research is

not merely of a theoretical nature. [165]

The fact that traffic analysis and data mining can be realistically performed using the retained traffic and location data is an aggravating factor to be considered. Adding to the severity of the interference with article 7 and article 8 of the Charter is the maximum retention period of two years with the possibility of further extensions in accordance with article 12. [166]

Lastly, when weighing the severity of the interference against the importance of the public purpose pursued by the Directive, the social harm potentially created by the Directive should also be considered. [167] To what extent will the Directive have a chilling effect on the exercise of people's fundamental rights? If behavioural modifications do ensue, what are the sociological effects? Would social minorities (based on political views, income class, religion, or any other factor) feel pressured to assimilate to the mainstream 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 deviating from what is considered appropriate by the majority? Few empirical data is available to answer these questions. They nevertheless should be considered in a determination of the Directive's proportionality.

Adequate and Effective Measures Against Abuse

The European Court of Human Rights has repeatedly held [168] that 'adequate and effective measures against abuse' need to be present in order for an interference to be proportional. Article 7 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, [169] which has been ratified by all Member States, [170] also mandates 'appropriate security measures' to protect the confidentiality, integrity, and availability of personal data. [171]

Article 7 of the Directive refers to the Data Protection Directive and the ePrivacy Directive 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 organisational measures [172] are to be employed to ensure the confidentiality, integrity, and availability of the retained data; (c) appropriate technical and organisational measures are to be used to ensure that the retained data can only be accessed by specially authorized personnel; [173] and (d) that data, except those that have been accessed and preserved, [174] shall be destroyed at the end of the period of retention. These measures and the ones to be implemented in accordance with the Data Protection Directive and the ePrivacy Directive could be considered 'adequate and effective' with regard to third parties (everyone except the provider and the national authorities) - that is if they are indeed implemented.

A lack of enforcement capabilities of the national supervisory authorities leading to insufficient outside review might severely limit the effectiveness of these measures. The national supervisory authorities referred to in article 9 will most likely not be able to effectively perform an individual security assessment for each provider. Framework Directive article 13b as amended by the Better Regulation Directive [175] will require new enforcement powers for national regulatory authorities: the power to issue binding instructions, [176] powers necessary to investigate cases of non-compliance, [177] and

the power to require providers to (a) provide information needed to assess the security and/or integrity of their services and networks, including documented security policies and (b) submit to a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the national regulatory authority, whereas the cost of the audit shall be paid by the provider. [178] These provisions, however, do not have to be transposed by Member States before May 25, 2011. [179] Until that date, they are of no direct relevance for the security of retained data and the proportionality of the Data Retention Directive. They do however clearly indicate the inadequacy of security measures currently required.

Another measure that would greatly add to the security of the retained data is an obligation to notify data security breaches to the individuals concerned. Such an obligation is provided for in article 4(3) ePrivacy Directive as amended by Citizens' Rights Directive. [180] However, this provision will also not have to be transposed until May 25, 2011. [181]

Furthermore, it has to be considered that a more centralized network infrastructure, as it is necessitated by the requirement to analyze all traffic, creates additional vulnerabilities. [182]

In addition to threats created by third parties, misuse by national authorities also poses a serious risk. It has to be emphasized that the Data Protection Directive does not apply to law enforcement agencies. [183] Given the standardisation efforts of the European Telecommunications Standards Institute (ETSI), [184] it seems likely that automatic data retrieval will soon be possible for national authorities. Article 10 of the Directive provides that Member States have to submit statistics on a yearly basis to the Commission. Reporting requirements generally have the potential to deter or to allow to detect (but not prevent) misuse by national authorities. However, according to article 14(1), article 10 is not meant to provide such a measure against abuse. [185] It should rather allow determining whether it is necessary to amend the list of data in article 5 and the periods of retention provided for in article 6.

Therefore, the security measures, as provided for by the Directive, cannot be considered sufficiently 'adequate and effective measures against abuse.' [186]

8. Conclusion

The Data Retention Directive clearly constitutes an interference with the fundamental rights to privacy and data protection. This interference is 'provided for by law' and serves the legitimate public purpose of supporting the 'investigation, detection and prosecution of serious crime.' Given this purpose, the Directive also has to be considered suitable and necessary. However, the Directive does not fulfil the requirement of proportionality *stricto sensu*:

It has been shown that the traffic and location data retention as mandated by the Directive is of limited effectiveness to facilitate the investigation, detection and prosecution of serious 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 telephony, fixed network telephony, Internet access, Internet e-mail, and Internet telephony, one simply has to choose an alternative means of communication. Internet

anonymising 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 but drastically increase the severity of the interference. Traffic analysis allows inferring much more information than is apparent from the retained data. This may include sensitive personal information such as one's medical condition, political affiliation, or sexual orientation. Social network analysis and data mining would especially allow for fishing expeditions [187] and a continuous surveillance of the entire population. People showing social patterns that are thought to be typical for a criminal or terrorist organisation might face more detailed analysis of their data or additional surveillance measures. In addition to the severity of the interference with an individual's rights to privacy and data protection, it can also be argued that the changes in society, potentially resulting from a constant surveillance, are contrary to the public purpose.

With a maximum as high as two years and possibilities of further extension in accordance with article 12, the retention period also seems excessive by any standard [188] and increases the severity of the interference with people's privacy.

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

In summary, the public purpose of the data retention is limited by the low effectiveness and the potential negative effects on society as a whole. It nevertheless constitutes a very severe interference with the fundamental rights to privacy and data protection but lacks effective measures against abuse. The interference therefore cannot be considered proportionate *stricto sensu*. Thus, the Data Retention Directive violates the fundamental right to privacy (Charter article 7) as well as the fundamental right to data protection (Charter article 8).

In the infringement actions brought by the Commission against various Member States for failure to transpose the Directive, the ECJ refused to consider the question of the legality of the Directive. However, in a case brought by the civil rights organisation Digital Rights Ireland to challenge the Directive's implementation in Ireland, the Irish High Court is expected to grant the plaintiff's motion for a reference to the ECJ under TFEU article 267, [189] forcing the ECJ to finally address the issue of whether the Directive conforms with the fundamental rights to privacy and data protection.

---

[1] Stanford-Vienna Transatlantic Technology Law Forum (TTLF); Research Fellow at the Forum on Contemporary Europe (FCE); Vice Director at the European Center for E-Commerce and Internet Law, Vienna.

[2] Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC). All unqualified

citations used in this text refer to this Directive.

[3] Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[4] Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

[5] For a general discussion of the conflict between privacy and the fight against crime and terrorism in the EU, see Gerhard Benn-Ibler, *Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten* [*Joint Fight Against Crime and Terror in Tension with the European Civil Rights*], 2008 Anwaltsblatt 12 (Austria). For a more international perspective, see Jeremy Warner, *The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps*, 2 University of Ottawa Law & Technology Journal 75 (2005).

[6] *See Commission proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, COM (2005) 438 final (Sept. 21, 2005).

[7] European Council Declaration on Combating Terrorism, 7906/04, at 5 (Mar. 25, 2004) (instructing the Council to examine 'proposals for establishing rules on the retention of communications traffic data by service providers')

[8] *See* European Council Declaration on the EU response to the London bombings, 11158/1/05 Rev 1, at 2 (July 13, 2005) (declaring that the Council's 'immediate priority' is to 'build on the existing strong EU framework for pursuing and investigating terrorists across borders' and further stating that it intends to adopt a framework decision on the retention of telecommunications data by Oct. 2005).

[9] Case C-301/06, Ireland v. Council and Parliament, 2009 E.C.R.

[10] Treaty establishing the European Community, Dec. 29, 2006, 2006 O.J (C 321 E) 37.

[11] Treaty of the Functioning of the European Union, May 9, 2008, 2008 O.J. (C 115) 47.

[12] *See* Case C-155/91, Commission v. Council, 1993 E.C.R. I-00939, § 19 (holding that recourse to EC Treaty art. 95 (now TFEU art. 114) is 'not justified where the measure to be adopted has only the incidental effect of harmonising market conditions'); Case C-187/93, Parliament v. Council, 1994 E.C.R. I-02857, § 25 (holding that 'the mere fact that the establishment or functioning of the internal market is involved is not enough to render [EC Treaty art. 95] applicable and recourse to that article is not justified where the act to be adopted has only the ancillary effect of harmonising market conditions within the Community'). Case C-376/98, Germany v. Parliament and Council, 2000 E.C.R. I-08419, § 84 (holding that 'a measure adopted on the basis of [EC Treaty art. 95] must genuinely have as its object the improvement of the conditions for the establishment and functioning of the internal market').

[13] Treaty on European Union, Dec. 29, 2006, 2006 O.J (C 321 E) 5.

[14] Case C-301/06, Ireland v. Council and Parliament, 2009 E.C.R.

[15] *Id.* § 84.

[16] *Id.* § 83. This finding also allowed the court to distinguish Case C-317/04, Parliament

v. Council, 2006 E.C.R. I-4721 which annulled Council Decision 2004/496/EC on the grounds that it regulated, for the purpose of public security, the transfer of flight passenger name records to the U.S. Department of Homeland Security. *Cf.* Spiros Simitis, *Übermittlung von Flugpassagierdaten* [*Transmission of Flight Passenger Name Records*], 2006 Neue Juristische Wochenschrift 2001 (Germany).

[17] Charter of Fundamental Rights of the European Union, 2007 O.J. (C 303) 1

[18] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Dec. 17, 2007, 2007 O.J. (C 306) 1.

[19] *See* EU Treaty art. 6 (ex EU Treaty art. 6) as amended by the Lisbon Treaty (stating that '[t]he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties').

[20] *See, e.g.,* Gerald Stampfel et al., Data Retention - The EU Directive 2006/24/EC from a Technological Perspective 41, 53, 103 (2008) (discussing Internet access, Internet e-mail, and Internet telephony but not fixed network telephony or mobile telephony). The only prior research that provides a somewhat similar technical analysis as presented in this article is only available in German and can be found in Lukas Feiler et al., Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmassnahmen im Bereich der Informations- und Kommunikationstechnologie [On the Way to the Surveillance State? New Information and Communication Technology Surveillance Measures] 126 et seq. (Wolfgang Zankl ed., 2009).

[21] Parliament and Council Directive 2002/21, 2002 O.J. (L 108) 33 (EC).

[22] *See* Int'l Org. for Standardisation [ISO], *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model*, ISO/IEC 7498-1:1994 § 6 (1994).

[23] 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* W. Richard Stevens, TCP/IP Illustrated, Volume 1 2 (1994).

[24] 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* W. Richard Stevens, TCP/IP Illustrated, Volume 1 2 (1994).

[25] For an introduction to VoIP and network convergence, see Analysys, *Final Report for the European Commission: IP Voice and Associated Convergent Services* (2004), *available at* http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/ip_voice/401_28_ip_voice_and_associated_convergent_services.pdf (last accessed Mar. 20, 2010).

[26] *See, e.g.,* Sven Gschweitl et al., *Voice over IP - Rechtliche Einordnung eines neuen Konzeptes* [*Voice Over IP-Legal Qualification of a New Concept*], 2005 Medien und Recht 503 (Austria).

[27] *See, e.g.*, Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 54 (Austria).

[28] Case C-211/09, Commission v. Greece, 2009 (holding that Greece had failed to transpose the Directive by Sept. 15, 2007).

[29] Case C-192/09, Commission v. Netherlands. On Oct. 9, 2009, the European Commission withdrew its application since the Netherlands had transposed the Directive after the commencement of the action. *See* Case C-192/09, Order dated Nov. 11, 2009.

[30] Case C-185/09, Commission v. Sweden, 2010 (holding that Sweden had failed to transpose the Directive by Sept. 15, 2007).

[31] Case C-189/09, Commission v. Austria, 2010 (holding that Austria had failed to transpose the Directive by Sept. 15, 2007).

[32] *Cf.* Reinhard Wolff, Keine Vorratsdatenspeicherung - Trotzige Schweden [No Data Retention - Defiant Swedes] (2010), *available at* http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/trotzige-schweden/.

[33] *See* Case C-189/09, Commission v. Austria, 2010, § 15 (referring to Case 226/87, Commission v. Greece, 1988 E.C.R. 3611, § 14; C-74/9, Case C-74/91, Commission v. Germany, 1992 E.C.R. I-5437, § 10; and Case C-196/07, Commission v. Spain, 2008, § 34).

[34] Commission Response to Access to Documents Request GESTDEM No. 2010/0018, JLS/F3/JV/WDK/mb D(2010) 2181, Feb. 15, 2010 (on file with author).

[35] Romanian Constitutional Court Decision no.1258 of Oct. 8, 2009, Official Gazette no. 798 of Nov. 23, 2009.

[36] The Federal Constitutional Court only stated that it is possible to transpose the Directive in a way that does not violate the Basic Law. The legality of the Directive was therefore not relevant to the decision. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 185 et seq.

[37] Grundgesetz für die Bundesrepublik Deutschland [GG] [Basic Law] May 23, 1949, Bundesgesetzblatt, Teil I [BGBl. I] 1, as amended.

[38] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08.

[39] *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 269 et seq.

[40] *See, e.g.,* Gerald Otto & Michael Seitlinger, *Die 'Spitzelrichtlinie': Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG* [*The Snitcher Directive: Regarding the (Transposition-)Problems of the Data Retention Directive 2006/24/EC*], 2006 Medien und Recht 227, 231 (Austria).

[41] However, there are also commentators who construe 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. This would effectively render the Directive useless with respect to Internet e-mail and Internet telephony-unless one regards all e-mail and VoIP service providers obligated to retain data. See Gerald Otto & Michael Seitlinger, *Die 'Spitzelrichtlinie': Zur (Umsetzungs)Problematik der Data Retention*

Richtlinie 2006/24/EG [*The Snitcher Directive: Regarding the (Transposition-)Problems of the Data Retention Directive 2006/24/EC*], 2006 Medien und Recht 227, 233 (Austria).

[42] *See, e.g.,* Rotraud Gitter & Christoph Schnabel, *Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht* [*The Directive for Data Retention and Its Transposition Into National Law*], 2007 Multimedia und Recht 411, 414 (Germany).

[43] *See, e.g.,* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 248 (2007).

[44] The structure of art. 5(1) is based on the six different data 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.

[45] 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.

[46] Art. 5(1)(c)(1).

[47] 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).

[48] The IMSI identifies the SIM card. *See* International Telecommunications Union [ITU], *The international identification plan for public networks and subscriptions*, ITU-T Recommendation E.212 (2008), *available at* http://www.itu.int/rec/T-REC-E.212-200805-I.

[49] The IMEI identifies a mobile phone itself.

[50] 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.' Pursuant to art. 5(1)(f)(2), data identifying the geographic location of cells also has to be retained.

[51] However, art. 3(2) explicitly allows 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* Gerhard Benn-Ibler,*Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten* [*Joint Fight Against Crime and Terror in Tension with the European Civil Rights*], 2008 Anwaltsblatt 12, 14 (Austria); Dietrich Westphal, *Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten* [*The Directive for the Retention of Traffic Data*], 2006 juridikum 34, 36 (Austria).

[52] Contrary to common sense, the obligation to retain the assigned IP address is codified in art. 5(1)(c) and not art. 5(1)(a).

[53] 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.

[54] Art. 5(1)(e)(3)(i) explicitly mentions 'dial-up access.'

[55] Art. 5(1)(a)(2)(iii).

[56] Art. 5(1)(c)(2)(i). Note that the Directive generally uses the term 'log-off.'

[57] 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 because the user is the one initiating the Internet connection.

[58] *See, e.g.*, Rotraud Gitter & Christoph Schnabel, *Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht* [*The Directive for Data Retention and Its Transposition Into National Law*], 2007 Multimedia und Recht 411, 411 (Germany).

[59] Art. 5(1)(a)(2)(i) and art. 5(1)(b)(2)(ii).

[60] Art. 5(1)(e)(3)(i).

[61] 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 referring to the sender of an e-mail. However, 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.

[62] Art. 5(1)(a)(2)(iii); Art. 5(1)(b)(2)(ii).

[63] J. Klensin, *Simple Mail Transfer Protocol*, RFC 5321 (2008).

[64] J. Myers & M. Rose, *Post Office Protocol - Version 3*, RFC 1939 (1996).

[65] M. Crispin, *Internet Message Access Protocol - Version 4Rev1*, RFC 3501 (2003). See below for a discussion of alternative mail transfer protocols, including web-mail.

[66] Art. 5(1)(d)(2).

[67] Art. 5(1)(a)(2)(i) and art. 5(1)(b)(2)(i). *Cf.* J. Rosenberg et al., *SIP: Session Initiation Protocol*, RFC 3261 § 19.1.3 (2002); Ted Wallingford, Switching to VoIP 150 (2005).

[68] 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.

[69] 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).

[70] Art. 5(1)(e)(3)(i).

[71] Art. 5(1)(e)(3)(ii).

[72] Art. 5(1)(c)(2)(ii).

[73] Art. 5(1)(d)(2).

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

[75] *See* Dietrich Westphal, *Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten* [*The Directive for the Retention of Traffic Data*], 2006 juridikum 34, 37 (Austria); Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 52 (Austria); Rotraud Gitter & Christoph Schnabel,*Die Richtlinie zur Vorratsdatenspeicherung und ihre Umsetzung in das nationale Recht* [*The Directive for Data Retention and Its Transposition Into National Law*], 2007 Multimedia und Recht 411, 412 (Germany).

[76] *See, e.g.,* Case C-317/04, Parliament v Council, 2006 E.C.R. I-4721, § 54.

[77] *See* Case C-301/06, Ireland v. Council and Parliament, 2009 E.C.R., § 83 (finding that '[t]hose matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive' which allowed the court to uphold the Directive).

[78] *Cf.* Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 53 (Austria). Not considering recital 25 and of a contrary opinion: Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 252 (2007) and Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 655 (2007).

[79] Directive art. 1(1).

[80] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 11, 1950, Council of Europe CETS No. 005, 213 U.N.T.S. 222.

[81] *See, e.g.,* Case C-274/99 P, Connolly v Commission, 2001 E.C.R. I-1611, § 37; Case C-260/89, Elliniki Radiophonia Tiléorassi v. Dimotiki Étairia Pliroforissis, 1991 E.C.R. I-2925, § 41.

[82] *Cf.* Joined Cases C-188/10 and C-189/10, 2010 ECJ EUR-Lex LEXIS 666, § 55 (referring to 'primary law, and in particular the rights recognised by the Charter of Fundamental Rights of the European Union, to which Article 6 TEU accords the same legal value as that accorded to the Treaties'). *See also* TFEU art. 267 (stating that the ECJ has not only the jurisdiction to give preliminary rulings on the interpretation but also the validity of 'acts of the institutions, bodies, offices or agencies of the Union'); TFEU art. 263 (giving the ECJ jurisdiction to 'review the legality of legislative acts [of the EU]').

[83] It is of course not a new concept that secondary EU law has to conform to fundamental rights that are part of primary EU law. *Cf.* Case 11/70, Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, 1970 E.C.R. 1125, § 4.

[84] *See* Charter art. 52(3) (stating that '[t]his provision shall not prevent Union law providing more extensive protection'). *Cf.* Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303) 33 (noting that '[t]he last sentence of [Charter art. 52(3)] is designed to allow the Union to guarantee more extensive protection').

[85] *See* Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303) 20. The Explanations are to be given 'due regard' when interpreting the charter. *See* EU

Treaty art. 6(1).

[86] *See, e.g.,* Joined Cases C-465/00, Rechnungshof v. Österreichischer Rundfunk, C-138/01, Neukomm v. Österreichischer Rundfunk, and C-139/01, Lauermann v. Österreichischer Rundfunk, 2003 E.C.R. I-4989, § 68 et seq.

[87] Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) § 41 (1978).

[88] *See, e.g.*, Jochen A. Frowein & Wolfgang Peukert, Europäische Menschenrechtskonvention [European Convention on Human Rights] art. 8, §§ 6, 34 (2d ed. 1996) (Germany).

[89] Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) § 84 (1984).

[90] Copland v. United Kingdom, 45 Eur. Ct. H.R. 253, § 43 (2007).

[91] Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303) 20 (noting that the word 'correspondence' has been replaced by 'communications' '[t]o take account of developments in technology').

[92] Amann v. Switzerland, 2000-II Eur. Ct. H.R. 247, § 65 (citing Leander v. Sweden, 116 Eur. Ct. H.R. (ser. A) § 48 (1987)).

[93] Copland v. United Kingdom, 45 Eur. Ct. H.R. 253, § 43 (2007). *Cf. also* S. and Marper v. United Kingdom, Eur. Ct. H.R., §§ 67, 121 (2008) (holding that '[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8' and that '[t]he subsequent use of the stored information has no bearing on that finding').

[94] *See* Charter art. 52(3).

[95] Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) § 67 (1984); Amann v. Switzerland, 2000-II Eur. Ct. H.R. 247, § 56; Rotaru v. Romania, 2000-V Eur. Ct. H.R. 156, § 55.

[96] For a general discussion of the requirement, see Yutaka Arai et al., Theory and Practice of the European Convention on Human Rights 337 (Pieter van Dijk et al. eds., 4th ed. 2006).

[97] Rotaru v. Romania, 2000-V Eur. Ct. H.R. 156, § 55.

[98] Like the ECHR, the Charter also refers to rule of law in its preamble (stating that the Union 'is based on the principles of democracy and the rule of law').

[99] 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.

[100] *See, e.g.,* Case C-331/88, Fedesa, 1990 E.C.R. I-4023, § 13; Joined Cases C-133/93, C-300/93, and C-362/93, 1994 E.C.R. I-04863, § 40.

[101] Charter art. 52(1).

[102] *Cf. generally* Roland Winkle, Die Grundrechte der Europäischen Union: System und allgemeine Grundrechtslehren [The Fundamental Rights of the European Union:

Framework and General Fundamental Right Theories] 267 (2006) (Austria).

[103] *Cf.* Stefan Ibing, Die Einschränkung der europäischen Grundrechte durch Gemeinschaftsrecht [The Restriction of European Fundamental Rights by Community Law] 337 et seq. (2006).

[104] Note that, once the EU has acceded to the ECHR, the European Court of Human Rights may review the Directive with regard to its conformity to the ECHR (but not to the Charter). *See* EU Treaty art. 6(2) (stating that '[t]he Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms').

[105] *Cf.* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, art. 5(b), Jan. 28, 1981, Council of Europe CETS No. 108, 1496 U.N.T.S. 66 (stating that personal data undergoing automatic processing shall be 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes'); Data Protection Directive art. 6(1)(b) (stating that Member States shall provide that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes').

[106] Treaty of the Functioning of the European Union, May 9, 2008, 2008 O.J. (C 115) 47.

[107] Charter art. 52(1). Art. 8 § 2 ECHR also specifically mentions 'national security' and 'the prevention of […] crime' as objective potentially justifying an interference.

[108] This is an issue that is considered with regard to the Directive's proportionality *stricto sensu*.

[109] *See* Dietrich Westphal, *Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten* [*The Directive for the Retention of Traffic Data*], 2006 juridikum 34, 38 (Austria).

[110] *See id.* at 36 (incorrectly assuming that HTTP-traffic data is also to be retained).

[111] *Cf.* Kevin Loney & Bob Bryla, Oracle Database 10g DBA Handbook 18 (2005).

[112] *See* Gerald Otto & Michael Seitlinger, *Die 'Spitzelrichtlinie': Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG* [*The Snitcher Directive: Regarding the (Transposition-)Problems of the Data Retention Directive 2006/24/EC*], 2006 Medien und Recht 227, 232 (Austria).

[113] *See infra.*

[114] *See, e.g.,* Case C-331/88, Fedesa, 1990 E.C.R. I-4023, § 14; Joined Cases C-133/93, C-300/93, and C-362/93, 1994 E.C.R. I-04863, § 42. *Cf.* Roland Winkle, Die Grundrechte der Europäischen Union: System und allgemeine Grundrechtslehren [The Fundamental Rights of the European Union: Framework and General Fundamental Right Theories] 278 (2006) (Austria). *Cf. also* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 207 (holding that suitability under German constitutional law only requires that the objective is furthered by the measures, noting that the various possibilities to circumvent the data retention are therefore irrelevant).

[115] '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 at the time the national authority wants access to the retained data, it has

to obtain a court warrant. *See* Dietrich Westphal, *Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten* [*The Directive for the Retention of Traffic Data*], 2006 juridikum 34, 38 (Austria); Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 249 (2007); Article 29 Data Protection Working Party, *Opinion 9/2004*, at 4, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf.

[116] *Cf.* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 208 (holding that 'quick freeze' does not provide a comparable tool for investigating crime).

[117] Arguing that traditional investigative measures are equally well suited and therefore constitute a 'less intrusive measure': Gerald Otto & Michael Seitlinger, *Die 'Spitzelrichtlinie': Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG* [*The Snitcher Directive: Regarding the (Transposition-)Problems of the Data Retention Directive 2006/24/EC*], 2006 Medien und Recht 227, 233 (Austria). This argument does not take into account that traffic analysis and social network analysis of the retained data can provide information otherwise unavailable.

[118] Note that only a few Member States have fulfilled their obligations under art. 10 to submit statistics on a yearly basis to the Commission. *See* Article 29 Data Protection Working Party, *Report 01/2010*, at 16 (July 12, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf. *See also id.* at 2 (noting that '[t]he lack of available sensible statistics hinders the assessment of whether the Directive has achieved its objective'). Individual cases are-despite being statistically irrelevant-often cited in support of the Directive. For example, the draft of the Commission evaluation which was leaked in May 2010 and, pursuant to article 14, should have been adopted by Sept. 15, 2010 refers to a number of such cases. *See Commission Room Document, Evaluation of Directive 2006/24/EC and of National Measures to Combat Criminal Misuse and Anonymous Use of Electronic Communications*, at 19 (2010), *available at* http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective20062 4EC.pdf).

[119] Dirk Wüstenberg, *Vorratsdatenspeicherung und Grundrechte [Data Retention and Fundamental Rights]*, 2006 Medien und Recht International 91, 96 (Austria).

[120] *Cf.* William Hugh Murray, *Security of Communication Protocols and Services, in* Information Security Management Handbook 2083, 2090 (Harold F. Tipton & Micki Krause eds., 6th ed. 2007) (discussing the Point-to-Point Tunneling Protocol and the Layer 2 Tunneling Protocol).

[121] For example, Google's mail service, Gmail, uses SSL encryption by default. *See* Ryan Singel, Google Turns on Gmail Encryption to Protect Wi-Fi Users (2010), *available at* http://www.wired.com/threatlevel/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users.

[122] RFCs are published by the Internet Engineering Task Force (IETF).

[123] P. Resnick, *Internet Message Format*, RFC 5322 (2008).

[124] J. Klensin, *Simple Mail Transfer Protocol*, RFC 5321 (2008).

[125] J. Myers & M. Rose, *Post Office Protocol - Version 3*, RFC 1939 (1996).

[126] M. Crispin, *Internet Message Access Protocol - Version 4Rev1*, RFC 3501 (2003).

[127] *See* Ted Wallingford, Switching to VoIP 119 et seq, 130 et seq. (2005).

[128] J. Rosenberg et al., *SIP: Session Initiation Protocol*, RFC 3261 (2002).

[129] ITU, *Implementors' Guide for Recommendations of the H.323 System (Packet-based multimedia communications systems): H.323, H.225.0, H.245, H.246, H.283, H.341, H.450 Series, H.460 Series, and H.500 Series*, ITU-T Recommendation H.Imp323/H.323 System (2009), *available at* http://www.itu.int/rec/T-REC-H.323/en.

[130] H. Schulzrinne et al., *RTP: A Transport Protocol for Real-Time Applications*, RFC 3550 (2003).

[131] For the significance of Facebook see Benny Evangelista, *Facebook directs more online users than Google*, S.F. Chron., Feb. 15, 2010, at D1.

[132] J. Oikarinen & D. Reed, Internet Relay Chat Protocol, RFC 1459 (1993).

[133] K. Murchison et al., *Netnews Article Format,* RFC 5536 (2009).

[134] C. Feather, *Network News Transfer Protocol (NNTP)*, RFC 3977 (2006).

[135] R. Fielding et al., *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616 (1999).

[136] Using custom key-value pairs submitted using the HTTP request method POST; *see* R. Fielding et al., *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616 § 9.5 (1999).

[137] Apparently of a different opinion: Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 52 (Austria).

[138] *Cf.* Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 56 (Austria).

[139] In certain configurations the commonly used mail server software qmail does exactly that. For example, if the author sends an e-mail using his provider's SMTP server mail.example.com to one of his colleagues at Empowered Media, the receiving mail server mx3.empoweredmail.com will only communicate with mail.example.com using SMTP over TLS. *See* Dave Sill, The qmail Handbook 264 (2002).

[140] Especially drug dealing organisations have been known to use pre-paid cell phones. *Cf.* Jelle van Buuren, *EU wants identification system for users of prepaid telephone cards* (2002), *available at* http://www.heise.de/tp/r4/artikel/12/12574/1.html (quoting an unpublished document of the Working Party on Drug Trafficking established by Council of the EU: anonymous prepaid telephone cards are 'one of the technological breakthroughs most widely used by criminal organisations').

[141] *E.g.* blocking cookies; *see* D. Kristol & L. Montulli, *HTTP State Management Mechanism*, RFC 2965 (2000).

[142] *Cf.* http://tor.eff.org (last accessed Mar. 20, 2010).

[143] *See* Roger Dingledine & Nick Mathewson, Design of a blocking-resistant anonymity

system (2007), *available at* https://svn.torproject.org/svn/projects/design-paper/blocking.html.

[144] *See* E. Rescorla, *HTTP Over TLS,* RFC 2818 (2000).

[145] *Cf.* Lukas Feiler, Tor als Prüfstein der Data Retention Richtlinie [Tor as the Touchstone of the Data Retention Directive] (2005), *available at* http://www.lukasfeiler.com/Tor.pdf.

[146] *See, e.g.*, Kevin Bauer et al., *Low-Resource Routing Attacks Against Anonymous Systems, in* WPES '07: Proceedings of the 2007 ACM workshop on Privacy in electronic society 11 (2007).

[147] S. and Marper v. United Kingdom, Eur. Ct. H.R., § 119 (2008).

[148] *Cf.* George Danezis, Introducing Traffic Analysis Attacks, Defences and Public Policy Issues … (Invited Talk) (2005), *available at* http://research.microsoft.com/en-us/um/people/gdane/papers/TAIntro.pdf.

[149] *See* Bruce Schneider, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2d ed. 1996) (defining cryptanalysis as the 'science of recovering the plaintext of a message without access to the key').

[150] Michael Herman, Intelligence Power in Peace and War 71 (1996).

[151] George Danezis & Richard Clayton, *Introducing Traffic Analysis*, in Digital Privacy: Theory, Technologies, and Practices 95, 109 (Alessandro Acquisti et al. eds., 2008).

[152] *See, e.g.,* Susan Trausch, *Pizza Politics*, Boston Globe, Aug. 30, 1991, Op-Ed section, at 15.

[153] *Cf.* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 211 (noting that the retained data might reveal social structures and decision processes within social groups and associations).

[154] *Cf.* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 211 (noting that the combination of the different kinds of retained traffic and location data allow the inference of detailed information about political affiliations, personal preferences, tendencies, and weaknesses).

[155] Pontus Svenson et al., *Social Network Analysis and Information Fusion for Anti-Terrorism, in* Proceedings of the Conference on Civil and Military Readiness 2006 (2006) (Sweden), *available at* http://www.foi.se/infofusion/bilder/CIMI_2006_S3_1.pdf.

[156] *Cf.* Dietrich Westphal, *Die neue EG-Richtlinie zur Vorratsspeicherung* [*The New EC-Directive for Data Retention*], 2006 Europäische Zeitschrift für Wirtschaftsrecht 555, 559 (also recognising the potential of data mining in the context of the Directive).

[157] *Cf.* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 615 (2007) (noting that mining the data is only one part of the process-the data must first be collected, generally from many different databases).

[158] Eurostat estimates that the total population of the EU, as of Jan. 1, 2010, was 501,259,840. *See* http://epp.eurostat.ec.europa.eu/tgm/table.do?

tab=table&language=en&pcode=tps00001&tableSelection=1&footnotes=yes&labeling=labels&plugin=1 (last visited Mar. 23, 2010).

[159] This is known as the base rate fallacy. *Cf.* Amos Tversky & Daniel Kahneman, *Evidential Impact of Base Rates, in* Judgment Under Uncertainty: Heuristics and Biases 153 (Daniel Kahneman et al. eds., 1985). *Cf. also* Douglas W. Hubbard, The Failure of Risk Mangement: Why It's Broken and How to Fix It 101 (2009) (referring to the problem as 'insensitivity to prior probabilities')

[160] *Cf.* Bruce Schneier, Why Data Mining Won't Stop Terror (2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357?currentPage=all. *Cf. also* Michael Blastland, A scanner to detect terrorists (2009), *available at* http://news.bbc.co.uk/2/hi/uk_news/magazine/8153539.stm.

[161] In particular, terrorism is not a phenomenon that is limited to a specific ethnic or religious group. *Cf., e.g.,* U.S. Department of Homeland Security, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment* (2009), *available at* http://www.fas.org/irp/eprint/rightwing.pdf (one of the report's key findings is that '[t]he possible passage of new restrictions on firearms and the return of military veterans facing significant challenges reintegrating into their communities could lead to the potential emergence of terrorist groups or lone wolf extremists capable of carrying out violent attacks').

[162] *Cf.* Ben Hayes, *Arming Big Brother: The EU's Security Research Programme, TNI Briefing Series No 2006/1* (2006), *available at* http://www.statewatch.org/news/2006/apr/bigbrother.pdf.

[163] 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* ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/i-tracs_en.pdf (last accessed Mar. 20, 2010).

[164] 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 € 1,132,895. The partners included EADS and the Swedish Defence Research Agency. *See* ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/hits-isac_en.pdf (last accessed Mar. 20, 2010).

[165] *See, e.g.,* http://www.industry.siemens.com/security/en/topics/proc_06_03.htm (last accessed Mar. 20, 2010, providing information regarding the Siemens 'Intelligence Platform'). *Cf.* M. Balser et al., *Überwachung made in Germany* [*Surveillance made in Germany*] (2009), *available at* http://www.sueddeutsche.de/politik/479/472998/text (reporting that the 'Intelligence Platform' had been sold to 60 governments).

[166] *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.' *Cf.* S. and Marper v. United Kingdom, Eur. Ct. H.R., § 119 (2008) (discussing the severity of indefinite data retention).

[167] *Cf.* Daniel J. Solove, Understanding Privacy 87 et seq. (2008) (arguing that when performing a balancing test, the social benefits of privacy should be primarily considered).

[168] Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) § 50 (1978); *see also* Rotaru v. Romania, 2000-V Eur. Ct. H.R. 156, § 59 (using the term 'safeguards' instead of 'guarantees'); *cf. also* Walter Berka, Die Grundrechte [The Fundamental Rights] § 466 (1999) (Austria).

[169] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe CETS No. 108, 1496 U.N.T.S. 66.

[170] *See* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG (last accessed Mar. 22, 2010).

[171] *Cf. also* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 222 (holding that 'data security is of great importance for the proportionality' of the retention of traffic and location data).

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

[173] This effectively means that the principle of 'least privilege' has to be employed. *Cf.* Simson Garfinkel et al., Practical Unix and Internet Security 235 (3d ed. 2003).

[174] This wording raises the question whether preserved data may never be deleted. *See* Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 54 (Austria). Art. 7(d) merely exempts said data from a minimum obligation to delete data. In conformity with the Data Protection Directive, national laws 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.

[175] Parliament and Council Directive 2009/140, 2009 O.J. (L 337) 37 (EC).

[176] Framework Directive as amended by the Better Regulation Directive art. 13b(1).

[177] *Id.* art. 13b(3).

[178] *Id.* art. 13b(2).

[179] *See* Better Regulation Directive art. 5.

[180] Parliament and Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC).

[181] *See* Citizens' Rights Directive art. 4.

[182] *See* Steven M. Bellovin et al., *Risking Communications Security: Potential Hazards of the Protect America Act*, 6 IEEE Security & Privacy 24 (2008).

[183] Data Protection Directive art. 3(2) explicitly states that data processing operations 'concerning public security, defence, State security […] and the activities of the State in

areas of criminal law' are outside the scope of the Data Protection Directive.

[184] *See* European Telecommunications Standards Institute [ETSI], *Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment*, ETSI TR 102 661 V1.2.1 (2009); ETSI, *Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data*, ETSI TS 102 657 V1.4.1 (2009); ETSI, *Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data*, ETSI TS 102 656 V1.2.1 (2008); ETSI, *Lawful Interception (LI); Retained Data*, ETSI TS 102 656 V1.1.1 (2007); ETSI, *Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications*, ETSI TR 102 503 V1.5.1 (2010).

[185] *Cf.* Doris Liebwald, *The New Data Retention Directive*, 2006 Medien und Recht International 49, 54 (Austria).

[186] Negating the presence of adequate and effective measures in general, i.e. without regard to the threat agent: Gerald Otto & Michael Seitlinger, *Die 'Spitzelrichtlinie': Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG* [*The Snitcher Directive: Regarding the (Transposition-)Problems of the Data Retention Directive 2006/24/EC*], 2006 Medien und Recht 227, 232 (Austria). *Cf.* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 224 (stating that the German Constitution does not require any specific security measures to be implemented but does require a particularly high degree of security for retained data that is 'state of the art' and should include a sophisticated encryption scheme, a secure access regime, e.g., by employing the four-eye principle and keeping audit logs).

[187] *Cf.* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 235 (2007) (stating that, in this information-rich environment, the danger of government fishing expeditions is extreme).

[188] 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: Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233, 251 (2007). 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.

[189] *See* Digital Rights Ireland v. Minister for Communication, Marine and Natural Resource, Draft Judgment/Ruling of Justice William M. McKechnie (May 5, 2010) (H. Ct.) (Ir.), *available at* http://www.digitalrights.ie/2010/05/05/high-court-decision-on-our-data-retention-challenge/.