

EXPERTS GROUP
"THE PLATFORM FOR ELECTRONIC DATA RETENTION FOR THE
INVESTIGATION, DETECTION AND PROSECUTION OF SERIOUS CRIME"
ESTABLISHED BY COMMISSION DECISION 2008/324/EC

SERIES A : GUIDANCE DOCUMENTS

Position Paper 4

Closer understanding of the term "third party networks and service providers" in relation to its application in Directive 2006/24/EC

Version 23 July 2009

Scope

This paper examines the role and responsibilities of third party networks and service providers to retain traffic data and subscriber information with regard to the obligations resulting from Directive 2006/24/EC.

Date and Status

- The Data Retention Experts Group provisionally adopted the document at its meeting of 16 March 2009, and asked for further comments.
- The current version was adopted in the meeting of 10 July 2009 and submitted for written procedure.
- A disclaimer applies (see at the end of the document)

Aspects of Directive 2006/24/EC covered in this paper

- The Directive applies to Public Electronic Communications Networks and Public Electronic Communications Services; these expressions are

defined by Framework Directive 2002/21/EC¹. Actors that do not provide such networks or such services do not fall within the scope of the Directive. The coverage of this paper is conditioned by that limitation.

- The Data Retention Directive requires that providers of "publicly available" electronic communications services and networks retain certain data² that are "generated or processed"³ by them.
- The Directive provides a number of aids to identify the provider that is obliged to retain data:
- Article 1 states that the aim of the Directive is to ensure that traffic data are available to fight serious crime. Its scoping provision states it only applies to communications data, and not to content;
- Article 3 of the Directive states who must retain traffic data, namely: providers of publicly available electronic communications services or of a public communications network. It limits the obligation to those data that are generated or processed by them in the process of supplying the communications services concerned, and moreover, in the case of unsuccessful call attempts, the data that they stored or logged.
- Article 5 specifies what data has to be retained.
- Recital 13 and 23 state that providers are only expected to retain data that are accessible and relate to their own services.
- Recital 13 also states that data should be retained in such a way as to avoid that they are retained more than once, rather than requiring that they are retained by each provider.

If the interpretation of the above requirements, and in particular of Article 3,

¹ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services OJ L 108/51 of 24 4 2002

² Directive Article 5

³ Directive Article 3 clause 1

leads to the conclusion that the Directive applies to a given third party network or service, the services or networks concerned must be considered as "publicly available" electronic communications services and networks.

Each service or network provider that is responsible to retain data according to the Directive must securely store the data and make them available at the request of competent authorities.

The interpretive aids also help to identify the responsible third party providers that are involved in the delivery of services to end-customers under a variety of commercial and business arrangements. Such providers are typically virtual network operators (VNO) and mobile virtual network operators (MVNO) that make services available as whole sale, outsourced or hosted.

The identification of providers that must retain data based on these aids requires a case-by-case approach.

Observations

Providers' networks often consist of infrastructures that are owned by different legal entities.

Services provided by these entities may be hosted or outsourced. In the case of MVNO, the network infrastructure is owned by a mobile network infrastructure provider, but the service itself is provided by the MVNO to its customers. In some cases where commercial arrangements exist between parties, no traffic data are retained. Subscriber information is typically held by the MVNO whereas the mobile network infrastructure provider avails of traffic data, although he has no business reason to capture and store them.

It follows from the Articles 1 and 3 of the Directive that both the service and the network providers must retain traffic data. Furthermore, the Directive stresses⁴ that traffic data must not be stored multiple times.

The delivery of an end-to-end communication service may not only

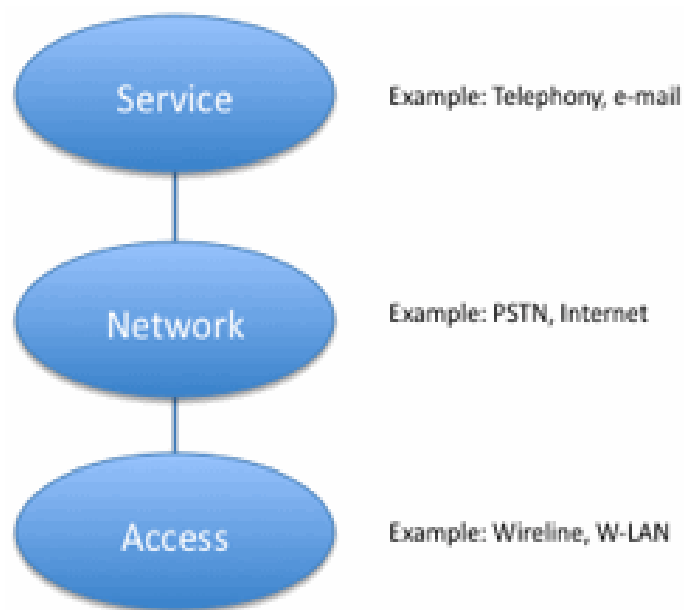
⁴ Directive Recital 13.

encompass different parts of a network but also involve several, and different, legal entities for instance where the network provider hosts or outsources the delivery of services on his network to third parties. The latter may own only be a part of the network and service infrastructure and not be in a direct commercial and/or contractual relation with the end-users.

The network operator (NO) supplies the production and controls the network. This usually includes most of the technical infrastructure and service platforms.

The VNO or equivalent department of a telecom operator that has a relation to the customer/end-user, relies in part or in its entirety on the Network Operators' production and support.

The Service Provider (SP) delivers one or several services directly or indirectly to the end-user. The SP often stands in a direct relation to the customer/end user including via commercial agreements.



A modern telecommunications system can be described as a three-layer model:

Each of these layers may be rendered separately, or in some combination, by different providers. The annex gives an example of a case in which the allocation of the responsibility to retain data is analysed.

Conclusions

Without special arrangements it may not be possible to provide law enforcement authorities (LEAs) with historical traffic data, in particular if parts of the provider's network are owned by different legal entities and services are hosted or outsourced.

An MVNO may not avail of the traffic data in connection with the service it provides to its customers. The MVNO typically has information about its customers but, depending on its business model, may not have any reason to capture and store traffic data. The mobile network infrastructure provider on the other hand, would typically have the possibility and resources to capture and store traffic data in connection with a 3rd party service (that is not his own service), but has no commercial reason or obligation to do so.

The identification of the actor that is obliged to retain data is especially challenging when several communication equipment assets are involved that are owned by different legal entities that have diverse business relationships with each other, and with the (end) customer of the communication services.

The obligation to retain traffic data falls on the network operator⁵ as well as on the providers that deliver the different kinds of services⁶ to end-

⁵ Directive - article 3 clause

⁶ Directive - recital 13 and 23

customers.

If third party networks and service providers are involved, the obligation to retain data according to the Directive is put on the provider of a "publicly available service"⁷, i.e. the legal "provider" who has a business relationship with the end-customer of the specific service that is delivered.

Details about subscriber data may not be available to the mobile network operator and vice versa, traffic data may not be available to the MVNO providing the service to the customer.

When evaluating the electronic communications market, it is practically impossible for service and network providers to avoid that the same traffic data is retained more than once.

From a law enforcement perspective, it is critical that traffic data is retained in a way that allows reconstruction of the communication (link). This means that it must be possible to correlate information from different providers.

Providers can be divided into the following categories:

NO – Network Operator

VNO –Virtual Network Operator

SP – Service Provider

When a Network Provider for example outsources wholesale voice, the equipment used to provide the service may be with the network provider, with the wholesaler or with another third party to which the wholesaler outsources the service.

In these situations, customer details must be correlated (linked or matched) with traffic data to reach the purpose pursued by the retention of data according to the Directive.

This may call for the integration of disparate systems and platforms from different providers that must be involved to get to the point where police

⁷ Directive Article 3.

can be provided with relevant data, even though not all providers are obliged to retain relevant (communication) data because they do not own the service.

The Directive states that a provider must only retain data relating to its own services⁸. Therefore, regardless of the complexities resulting from the involvement of third party networks and services, the “provider” of the service, i.e. the “service owner”, must retain the data.

Moreover, in scenarios where customer details are held by one, and the call data records by the other party, and where integration of both sets of data is necessary to compile the full set of data, it is most likely that the platforms, interfaces and data formats are different. Integration thus requires significant system management, between different third party networks and service providers.

Recommendations

An assessment should be made of the data that are available under normal operating business conditions⁹ in all those cases where networks consist of different elements that make up the infrastructure to deliver end-to-end services and where these elements are owned or controlled by a number of different third parties.

Only the data that is processed and stored under the normal conditions of operating the relevant business should be retained in accordance with the obligations defined by the national law transposing the Directive, and, if requested, be provided to LEAs.

The “provider” may need to give consideration to include an agreement on the collection and storage of traffic data in their commercial contracts with the third parties.

LEAs should assess on a case-by-case basis what traffic data and customer information is available and from which entity under normal

⁸ Directive Recital 13 & 23

⁹ Directive Article 3

business operations. Moreover, they must be prepared to request data from more than one entity and to correlate the data that is stored in and retrieved from separate locations.

MVNO shall retain the data they store under normal business conditions, i.e. the subscriber information and make this available to LEAs in accordance with the obligations defined by the national law transposing the DRD. Where an MVNO stores (retains) traffic data or outsources the storage to a third party (i.e. the mobile network infrastructure provider) as part of the normal operation of its business, then such data shall be made available to LEAs.

Providers of services offered separately “on top of” network access and Internet connectivity have to individually fulfil their obligation to retain data for their own services under the DRD.

Care must be taken not to store data more than once, thereby recognizing that in complex scenarios and networks the coordination for retention of traffic data may not be possible.

Disclaimer

The views and opinions expressed in this document are not necessarily shared by all Members of the Expert Group "the Platform for Electronic Data Retention for the investigation, detection and prosecution of serious crime" and do not constitute legal advice.

For details about the origin and status of the guidance contained in this document refer to the accompanying document "Introduction to the Series".

The opinions expressed in this document do not necessarily reflect the views of the European Commission which accepts no responsibility or liability whatsoever with regard its contents.

Appendix A: General scenario for hosted and outsourced services

The different providers involved in offering a communication service to the end-user may need to have an agreed relationship with each other to ensure that the combination of equipment used to deliver the service also enables the retention of traffic data resulting from the communication.

The following examples present the basic complexities for third party providers of wholesale, hosted and outsourced services to retain traffic data according to the Directive.

Examples:

- A GSM/3G subscriber may be using a suite of services:
 - ♦ Mobile phone telephony in the GSM/3G network including SMS
 - ♦ Mobile Internet access, GSM/3G IP connectivity with WiFi/hotspot as alternative
 - ♦ MMS over an IP network
 - ♦ VoIP (Voice over Internet) services provided by a third party or the network operator
 - ♦ E-mail services

- MVNO services:

The Mobile Network Operator has a commercial relationship with a third party fixed network operator to allow the mobility of their services (i.e. Mobile Virtual Network Operator) over its mobile network access infrastructure. In this case, depending on the cost/business model, the mobile network operator may hold details of the data traffic when a communication takes place but the subscriber details are held by the MVNO that owns the relationship with its customer. As this is not the mobile network provider's own service but that of the MVNO, the obligation to retain data is with the MVNO. As no traffic data are logged, traffic data is not available from the MVNO contrary to its customer's subscriber details that are available.

- WiFi "hotspots"

The Mobile Internet (Access) Service Provider enables the IP traffic services. Provided the terminal has the capability, WiFi can be an access alternative from various providers through "hotspots".