

# Expert Statement

European Working Party on Information Technology Crime  
Interpol

---

## Overview of vital traffic data necessary for investigations for which the EWPITC asks the general retention by telecommunication operators and telecommunication access and service providers

---

The European working party on Information Technology Crime is a workgroup that was established in 1991 that is hosted and supported by Interpol. It is composed of police officers and experts of specialised computer crime units of 12 states in the European Interpol Region. The members of the EWPITC come from the following countries : Austria, Belgium, Denmark, France, Finland, Germany, Italy, Netherlands, Portugal, Spain, Sweden, and United Kingdom.

This document does not represent the official view of Interpol or of any of the countries that are represented in the working party.

***It is a critical overview of vital traffic data that is needed for cyber crime investigations and for which the EWPITC asks for a general retention for no less than 12 months.***

***It is based on a discussion and the compilation of requirements expressed by expert cyber crime investigators with many years of experience.***

Content of this document

- 1. The essential need for general data retention***
- 2. General view on data used by investigators in cyber crime investigations***
- 3. Conceptual approach to determine the traffic data to be retained***
- 4. Retention periods***
- 5. Conclusions and request for co-operation***

***Annexes***

***Contact persons***

## 1. *The essential need for general data retention*

-----

To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities need to use traffic data <sup>(1)</sup> stored or used by telecommunication operators, telecommunication access and service providers.

*Wherefore will the traffic data be used ?*

The **ultimate goal** of the general data retention is to be able in case of a crime :

- to **trace back** and
- **locate** geographically and chronologically
- the **end user device** that was used to transmit the initial information.

This should be possible regardless of whatever kind or combination of telecommunication technologies and services were used.

*Why do we need this traffic data ?*

Firstly, this new telecommunication technologies give anyone the possibility of **controlling and operating from a distance** not only computer and telecommunication systems but also machinery and equipment. These operations can and in most case will have an effect in the “real” world.

But, the acting person is not physically present any more at the place where the effect is taking place. So ... there **are no physical traces any more** – no fingerprint, no footsteps ... nothing, **except telecommunication trails**.

Erasing these trails would have the same effect as wiping all fingerprints and bloodstains in the scene of bloody murder, before any police investigations could start.

Furthermore the actual telecommunication technologies and services allow anyone to connect and communicate very anonymously from nearly any place in the world. **A lot of information is also unreliable** because of the very common use of nicknames and aliases. So if the identity data provided by the end user can no longer be trusted, Law Enforcement has to fall back to **data that can not be tampered with by the end user** : telecommunication traffic data.

*Is real time collection of traffic data from the moment of the discovery of the crime not enough for investigators – thus avoiding keeping log files of traffic data ?*

As in real life, a lot of cyber crime is perpetrated once and not repeated afterwards. Starting to collect data after the discovery of those crimes does not help anymore – the perpetrator is not coming back. So, in those cases we will not find new traces to our target by real time collection of traffic data.

*Is an expedited preservation of traffic data not enough for investigators ?*

In a lot of ICT crimes and abuse of ICT systems for criminal purposes, the criminal seeks not to be detected so that he can continue to abuse the victim’s ICT system.

In many cases they succeed in doing so and it is only after some time – sometimes months- that the crime is detected. Expedited preservation of traffic data will in those cases very often be in vain. Think of the free or flat rate telecommunication services for which no traffic data is needed for billing purposes.

---

<sup>1</sup>() Traffic data : information elements on the signal/data transmission needed to realise or to control the telecommunication.  
This information does not include the content of the telecommunication.

## 2. General view on data used by investigators in cyber crime investigations

---

In the process of criminal investigations in a digital environment a distinction can be made to five categories of data of which the police could need to have on a certain moment access to.

1. Subscriber or administrative data (user password, name, address etc.)
2. **Traffic data** (log-in, cli, IP address, location etc.)
3. Content data (the content of e-mail messages, webpages, ftp-files etc.)
4. Transaction data (data about selling/order goods / invoices / services / etc.)
5. Payment data (buying/money transfer etc.)

We state that for the start of any investigation some traffic data needs always be available. Without these data it is impossible to investigate or collect any other evidence information needed<sup>(2)</sup>.

In this document we will focus on the category of traffic data and try to establish an approach to determine and catalogue the traffic data to retain.

## 3. Conceptual approach to determine the traffic data to be retained

---

This conceptual approach can be useful to get a view and an understanding on where data is stored and why law enforcement needs this information. It can be used in a general way for all telecommunication services (existing and future). The exact definition of the traffic data that has to be retained, results from the use of this approach but has to be written down more explicitly for the sake of a clear legal position of all parties concerned.

### 3.1 A layered approach (see also annex 1)

In our approach to determine the traffic data that has to be retained, we have structured our requirements in three levels, very similar to way telecommunication networks are structured :

Level	Description	Examples
1	Data/Signal carrier	Fixed telephone, cable connection, satellite, etc.
2	Data network	Internet access and networking (protocols IPv4 / IPv6) etc
3	Service application	E-mail, Web mail, Web publications, newsgroups, SMS gateways

In each layer the telecommunication operator or provider uses different **elements to identify the source and the destination** of the telecommunication.

Level	Description	Examples
1	Data/Signal carrier	Called number, calling number, IMEI, cable modem ID, MAC,
2	Data network	IP addresses of source and destination (v4 or v6), NUI, ...
3	Service application	E-mail addresses, Web mail, Web publications, newsgroups, SMS gateways

---

<sup>2</sup> () Please note that without these data nor the most simple criminal case (spread of viruses or child porn) nor the most serious criminal case (hacking, organised crime, threats on life and health, terrorism etc.) can be solved.

To be able to establish the complete telecommunication, there are on level 2 and 3 traffic data elements that make the **link with the immediate underlying level**.

At level	Information on level	Examples
2	1	Calling number, cable modem ID, MAC
3	2	IP-address of sender of mail, of web uploader, ...

We are aware that the delivered service at these three levels, can be with different companies :

- telecommunication operators and data carrier operators
- Internet access providers
- telecommunication service providers.

To be able to trace back a telecommunication to the physical device, the traffic data available at each of these companies has to make a complete chain.

### 3.2 Vital and significant traffic data

We consider as **VITAL DATA** : the traffic data without which information no cyber investigation can be started or continued to the end.

The EWPITC states that have to be considered as vital and thus have to be retained the following traffic data:

- **for connections to the data carrier (level 1) and to the data network (level 2)**
- **the identifying elements of the source and the destination of the communication**
- **the data and time of the connection**

Depending on the importance of the used telecommunication service applications, traffic data for those services can also be considered as VITAL.

We consider as **SIGNIFICANT DATA** : traffic data that is of great significance to the police's ability to solve very serious crime cases like murder cases, organised crime and terrorism, if they are recorded and stored by suppliers of computer and telecommunication services. Other elements in the traffic data at level 1 and 2 can also be considered as significant.

In **annex 2** we have made an overview of the traffic data for most important telecommunication technologies and services for which the EWPITC considers the retention vital or significant. The technical details have to be further verified with the concerned parties : LE and telecommunication industry.

### 3.3 New emerging technologies and services

The cyber world is one of quickly evolving technologies and services, so it is impossible to be complete when we catalogue the traffic data which we consider as vital today.

Based on the above concept, it has to be clear for all parties concerned what traffic data should be considered as VITAL and for which data retention is needed. Developers, operators and providers should consider these requirements when developing or implementing new technologies and services.

## 4. Retention periods

-----

As EWPITC we ask for a minimum retention period of 12 months for vital traffic data.

Taking into account the importance of combating serious organised crime, a longer retention period up to 24 months should be considered for some categories of vital or significant traffic data.

*Why aren't 6 months enough as retention period ?*

A retention period of 6 months as mentioned in some proposals of different countries, seem to short for the members of the EWPITC.

Besides the need for data retention in traditional and organised crime, this information is vital in the combat against ICT crime like hacking, sabotage, illegal copying of information, and so on. These crimes can resort very serious consequences and, as far as we can establish at this moment, they are a real danger to privacy of all telecommunication users.

In this kind of crimes there is in most cases nothing else than the logs of telecommunication systems to trace back our criminal.

Where in some cases a retention period of 6 might seem very long, it surely is insufficient for the combat of ICT crime.

In most cases there is a **phase of preparation** during which the ICT system of the victim is searched for vulnerabilities. The discovered vulnerabilities of the victims ICT systems are not always immediately abused. In some cases this only happens months later. (e.g. PABX abuses)

When the cyber crime actually took place, it is **not always immediately discovered** by the owner of the attacked computer system. It may well take months before the owner realizes he has been hacked, in which case it can be very difficult to trace back in time the initial attack during which a backdoor was installed on a computer system.

When the owner does discover the cyber crime, he often takes his **time to considering if he will or not make a complaint**. And then when has decided to make the complaint, it is not always immediately with the right police unit, and it can take **some time before the specialised police unit gets involved** in the investigations. Now, these units, like in other ICT branches lack often personnel so they have to handle cases one by one prioritising them according to their seriousness and possible prejudicial consequences.

In ICT crimes the use of **several intermediate systems** or “stepping stones” to reach the final targeted computer system is very common. Cyber criminals often use free subscriptions, free Internet accesses at universities, cyber cafés or even pirated subscriptions or hacked computers. These intermediate computer systems may and very often do lay **in different countries**. Getting the needed traffic data in each country with **rogatory letters can take quite some time**. So, if the hacker uses a chain of hacked systems to reach his targeted system it might take some months before we get to “source” of the attack.

Now, as it is not possible to make the distinction between telecommunications during which cyber crimes are being committed, and normal telecommunication use, it is imperative that the **retention period of vital “traffic data” is set to minimum 12 months**.

## **5. Conclusions and request for co-operation**

---

As a summary, traffic data is essential for tracing perpetrators in all types of cases, with mainly the focus on:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li><input type="checkbox"/> breaking into computer systems (hacking)</li><li><input type="checkbox"/> theft of trade secrets</li><li><input type="checkbox"/> sabotage of critical IT systems</li><li><input type="checkbox"/> abuse of telephone systems (phreaking)</li><li><input type="checkbox"/> theft of telephone units</li><li><input type="checkbox"/> fraud</li><li><input type="checkbox"/> drugs trafficking</li><li><input type="checkbox"/> human smuggling</li></ul> | <ul style="list-style-type: none"><li><input type="checkbox"/> threats on life and health</li><li><input type="checkbox"/> blackmail</li><li><input type="checkbox"/> harassment and defamation</li><li><input type="checkbox"/> terrorism</li></ul> |
|---|--|

The European Working Party on Information Technology Crime of Interpol asks all countries from the European Union and abroad :

- to recognise the need of retention of vital and significant traffic data for investigations
- to support the presented conceptual approach to determine the traffic data to retain
- to agree on the retention of vital data on level 1 & 2 for a period no less than 12 months**
- to consider the retention of other traffic data as far as it is indicated as significant in this document**

All parties are invited for constructive remarks on :

- social, political, economical and technical feasibility
- technical proposals to prevent eventually the need for data retention

### **Annexes**

-----

1. Scheme of the conceptual approach to determine the traffic data to retain
2. Catalogue of traffic data version 27-11-2001

### **Contact persons**

-----

#### **EWPITC**

**Luc Beirens**, Belgian Federal Police, Federal Computer Crime Unit,  
Direction for combating Financial and Economical Crime  
Notelaarstraat 211, B1000 Brussels Belgium+32 2 743 74 74

**Richard Vriesde**, Netherlands, Progambureau Digital Investigations,  
Nathaliegang 241, Postbus 7045 2701AA Zoetermeer Netherlands

#### **Secretariat General of Interpol**

**Michael Holstein**, High Tech Crime Unit, Interpol General Secretariat  
200, quai Charles de Gaulle, 69006 Lyon, France, Tel. +33 472 44 7221