Ministry of Security and Justice

Central Information Point for Telecommunications Investigation

(Centraal Informatiepunt Onderzoek Telecommuncatie, CIOT)

Contributing to law enforcement and security in the Netherlands

In the Netherlands both in front of and behind the scenes work is being carried out on the security of citizens and our country. (Special) Investigation, Intelligence and Security Services are active to prevent criminal or terrorist activities and to track down persons suspected of a crime. Sometimes they need information for these investigations from providers of telecommunication and internet services.

Telecommunication and internet providers are obliged by law to make the telecom and internet information of their clients available for the purpose of investigation. This is stipulated in the *Besluit verstrekking gegevens telecommunicatie* [Telecommunications (Provision of Information) Decree]. The data involved concerns personal information, address data relating to telephone numbers, IP addresses and e-mail addresses.

The CIOT is responsible for the careful storage and use of these data according to the legislative frameworks. CIOT stands for *Centraal Informatiepunt Onderzoek Telecommuncatie* (Central Information Point for Telecommunications Investigation). The CIOT manages the automated CIOT information system (CIS), in which the request-and-response traffic is handled quickly, smoothly and with due care. In other words, the CIOT acts as an intermediary between services requiring information and the telecom and internet providers that can offer this information. Through the CIOT providers make their contribution to a just and safe society.

The Central Information Point for Telecommunications Investigation (CIOT)

The CIOT was established in implementation of the Telecommunications (Provision of Information) Decree. Providers of telecommunication and internet services must provide business data to the CIOT on the users of their services. The fully automated CIOT information system (CIS) streamlines requests for information and responses to these. The CIOT itself does not examine the data; instead it is responsible for managing the CIS and in this way contributes to careful storage and use of the information. The CIOT reports each year to the Minister of Justice on the use of the system.

The objective of the CIOT is to make a contribution to a just and safe society. The information point wants to play a (pro) active role in the business process of the (Special) Investigation, Intelligence and Security Services by making the data provided available in an efficient, safe and structured manner. The CIOT carries out this task with due observance of the rules and restrictions laid down by law.

Law enforcement and national security

The CIOT was set up to make the information requests from (Special) Investigation, Intelligence and Security Services and responses to these requests by telecom and internet providers easier, independent of volume and safer. Market forces in the telecommunication and internet sector result in an ever increasing number of providers of these services. To avoid the authorised authorities having to keep in contact with all the providers, the CIOT information system was developed as a central service that handles all request-and-response traffic automatically.

The importance of telecom and internet information in investigations is increasing and this means that the CIOT information system is consulted more and more by the authorised authorities. They are heavily involved in tackling criminal activities and the protection of national security. During an investigation of this nature it is very important to be able to determine the identity of a suspect. Name and address data, for example, can be obtained from a telephone number on a mobile phone that is registered with a telecom provider.

Operating within the legislative frameworks

In the performance of its duties the CIOT must comply with various laws and decrees, as do the providers of telephony and internet information and the services that request the information. The Telecommunications (Provision of Information) Decree is the basis for the work of the CIOT. This decree elaborates on article 13.4 of the Telecommunications Act and stipulates that providers of telecommunication and internet services must provide information on their clients in certain circumstances.

The decree also regulates that the data must be provided automatically via a central information point (the CIOT) to the (Special) Investigation, Intelligence and Security Services. The information may only be requested by authorised authorities. The CIOT itself may not store files for purposes other than its statutory tasks, but must keep data on the use of the system for an annual audit and reports to the Minister of Justice.

The (Special) Investigation, Intelligence and Security Services may only request information from the CIOT for prosecution, collection of intelligence or provision of assistance in emergency situations. This is laid down in the Dutch Code of Criminal Procedure, the *Wet op de Inlichtingen- en Veiligheidsdiensten in Nederland* [Dutch Intelligence and Security Services Act] and the *Telecommunicatiewet* [Telecommunications Act].

The *Wet bescherming persoonsgegevens* [Personal Data Protection Act] applies to the data that are requested via the CIOT information system. Because this act is so important – after all, the information recorded is of a sensitive nature – the CIOT consults regularly with the Dutch Data Protection Authority to coordinate the operation of the CIS.

Careful checks

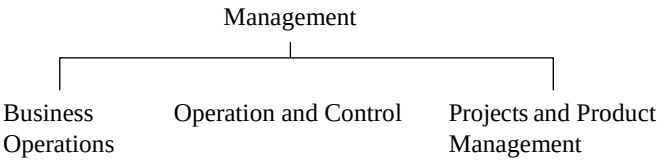
The work of the CIOT and the use of the CIOT information system are subject to regular checks. This is also laid down in the Telecommunications (Provision of Information) Decree. An audit must be carried out every year at the CIOT, the providers and requesters. During this audit it is verified whether the work has been carried in accordance with the legislative frameworks and that the providers supply the correct information to the CIOT. The audits are commissioned by the Ministry of Security and Justice and discussed in the CIOT Advisory Committee, on which the ministries concerned, the providers and requesters of information and other important stakeholders are represented.

The CIOT reports in an annual report to the Minister of Justice on the number of times the authorised authorities have received information via the CIOT within the framework of the investigation of criminal offences. The report states how often information has been provided through the medium of the CIOT, what the legal basis was for each request and which (Special) Investigation Service made the request.

Organisation of the CIOT

The CIOT is part of the Ministry of Security and Justice and comes under the Administration of Justice and Law Enforcement Policy Instruments Department (DIRR) of the Directorate-General for the Administration of Justice and Law Enforcement. The CIOT was set up in 1999.

Organisational chart



Statutory provision of information by telephony and internet providers

Since 1 September 2004 providers of public telecommunication networks and/or services are obliged by law to make the business data of their clients available to the CIOT. As of 1 September 2006 this obligation also became applicable for providers of public internet networks and/or services.

The CIOT ensures that providers are connected to the CIOT information system. Each provider must then provide an up-to-date digital file every 24 hours. They receive compensation for this from the government.

The file contains the following information on persons who make use of the network/the service of the provider:

Telecommunication providers	Internet providers
Name, address, postcode, town	Name, address, postcode, town
The telecommunication service of the user (fixed line, mobile, subscription, prepaid, etc.)	The internet service of the user (dial-up, cable, ADSL, e-mail account, etc.)
Telephone number(s) of the user	Identification numbers of peripheral equipment of the user, IP addresses, e-mail address(es) of the user, user name or log-in name
Name of the telecommunication provider	Name of the internet provider

Agreements

Providers must fulfil a number of technical, legal and administrative conditions. This ensures the protection of the data and the guarantee of privacy, among other things. In turn the CIOT enters into three agreements with each provider.

- The processor agreement is concerned with the responsibility for processing the information within the framework of the Personal Data Protection Act. In this way the CIOT ensures, among other things, that the data of the provider are kept in a separate, secure environment and that they are only used for the lawful provision of information.
- The audit agreement contains agreements on the annual check on the lawful use of the information system and the check on the correctness of the data provided.
- In addition, the CIOT enters into a Service Level Agreement with each provider so that it is clear what the provider can expect from the CIOT and how this is organised.

Fully automated from request to response

The CIOT ensures that providers of telecom and internet services and the authorities that can request the information are connected to the CIOT information system. A simple, transparent process from request to response then starts that is fully automatic per computer - and is therefore efficient and cost effective.

Space is reserved for each provider file in one of the *black boxes*: a secure environment in which the provider stores a file once every 24 hours with the statutory client data. Because the black box is a secure environment, the various providers cannot access one another's files.

The requestors have direct access 24 hours a day, seven days a week to the information system via their own *client application*. Only authorised authorities may make information requests. The Minister of Justice has granted this authorisation to the more than 40 (Special) Investigation, Intelligence and Security Services. They are given a special access code for this and may then only ask specific questions within the framework of the investigation.

The requester enters his information request on the client who passes it to the *server* at the CIOT. The request is made anonymous on the server. The request is sent to all black boxes where it is checked automatically whether the requested information is present. The provider cannot check which requester made the request and for what specific purpose which request was made. The response is returned to the server that passes it to the client of the requester. So that this all takes place in a secure manner use is made, among other things, of a closed network and encryption by means of a Public Key Infrastructure (PKI). The whole process takes a maximum of ten seconds, a considerable improvement compared with the previous method of sending questions by fax.

Lawful use

The CIOT is responsible for the technical management of the infrastructure, the maintenance and the development of the system. It also stores process information that can be used to check the lawful use of the system. This is information that shows by which provider, to which authority and on which legal basis information has been provided. Pursuant to the Telecommunications (Provision of Information) Decree, the CIOT is obliged to collect this process information for the annual audits and the reports to the Minister of Justice. This information expressly does not concern the content of the information. That information is only visible to the requester himself. The CIOT does not have a central database, but several *black boxes*, from which the data are provided exclusively by means of the request-and-response process.

Cooperation and coordination

The CIOT organisation is as independent as possible and works closely with the ministries involved and associated organisations. In addition to the Ministry of Security and Justice, the Public Prosecutor and the judiciary, it cooperates with the Ministry of Economic Affairs (EZ) and the National Telecom Agency, the Ministry of the Interior and Kingdom Relations (BZK), the Ministry of Defence, the Ministry of Agriculture, Nature and Food Quality (LNV), the Ministry of Housing, Spatial Planning and the Environment (VROM), the Ministry of Finance, the Ministry of Social Affairs and Employment (SZW) and the Dutch Data Protection Authority.
Together with the providers and requesters and other important stakeholders, the Ministries of Justice, Economic Affairs and the Interior and Kingdom Relations are represented on the CIOT advisory committee. The committee commissions the annual audit, evaluates the operation of the CIOT and makes recommendations on this. It also issues advice with regard to improvement of the information system and the development of additional functionalities.

The providers and authorised authorities who request information have cooperated in the development of the CIOT information system. They are also consulted regarding the maintenance of the system. For example, during the national user day that the CIOT organises each year for the requesters, or during the information meetings that are organised with the providers.

Telephony and internet information helps to solve crimes

Over 40 authorised authorities may use the CIOT information system to request telecom and internet information within the framework of investigation. These are:

- *Investigation services*: the regional police, units of the National Criminal Intelligence Service, the Central Criminal Intelligence Division, the Royal Marechaussee (KMAR), the National Police Services Agency (KLPD) and the National Prosecutor's Office.
- *Special investigation services*: the Fiscal Intelligence and Investigation Service (FIOD), the General Inspection Service (AID), the Intelligence and Investigation Service (IOD) and the Social Security Intelligence and Investigation Service (MIVD).
- *Intelligence and Security Services*: the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD).

Practical examples

Telephony or internet information may help to get investigations, which have reached an impasse, going again. An example is an investigation into a murder, in which all the leads had been followed without resulting in new information. The competent authority then decided to request the traffic data from the transmitting masts for mobile phones in the vicinity of the place of the crime on the day of the murder. This resulted in more than 30,000 telephone numbers that were queried via the CIOT at telecommunication providers. Analysis of the information obtained in this manner resulted in new information and the murder suspect was finally arrested.

Central Information Point Investigation (CIOT)
Schedeldoekshaven 131
P.O. Box 484 | 2501 cl Den Haag
t (070) 370 33 10
info.ciot@ibo.justid.nl
www.ciot.nl

The Ministry of Security and Justice:
working towards a safer society

Publication number: j-14522