

Summary

The Dutch implementation of the Data Retention Directive

On the storage and use of telephone and internet traffic data for crime investigation purposes

The study: background, research questions and data collection

Background to the research questions

The Dutch implementation of the Data Retention Directive was adopted at the 1th of September 2009. The main reason for the storage of call detail records of telephony and internet traffic data is that the data may be helpful in the investigation and prosecution of serious crimes. This data can be used, for example, to ascertain the time and place at which a certain mobile telephone was used to make a call. It is also possible to find out whether and when a computer or mobile telephone made an internet connection. Telecommunication traffic data can be used in cases involving a crime that merits pre-trial detention, a reasonable suspicion of a crime being planned or committed in an organised context and indications of a terrorist offence. However the fact that this data has to be stored for a certain period of time is a recurring point of debate. There is a need both in the Netherlands and at European level (EU 18620/11) for a clearer understanding of how the police and judicial authorities use the data kept under the Telecommunications Data (Data Retention Directive) Act (referred to below as 'the Act').

The purpose of this study is to clarify how the Act works in practice. This study does not strictly take the form of an evaluation. It extends beyond the scope of a process evaluation (cf. Wartna, 2005; Nelen et al., 2010), because there is a need not only for an understanding of how the Act has been shaped in practice but also of how the data to be kept available under this Act is actually used for criminal investigations in practice.

It is not however possible – as it would be in a product or effect evaluation – to ascertain how the introduction of the Act has affected the use of traffic data in criminal investigations. The telecommunication data at issue here was already available for criminal investigation purposes before the Act was introduced, and was already being used in criminal investigations into serious crimes prior to the introduction of the Act.

Although the Act has resulted in the retention periods being harmonised, the fact that other changes have taken place in the meantime means that it is only barely possible to measure and identify the effects of this. Changes in how telecommunication data is used in practice can be attributed primarily to the emergence of the mobile telephone and the smartphone and to the ability of people to use the internet to communicate with each other. It is

therefore possible to look into how telecommunication data is used in criminal investigations, but it is less easy to relate the findings to the introduction of the new Act.

This study focuses both on questions about how the Act has been given shape and questions about how the retained data is used in practice.

Various organisations and parties are involved in storing, maintaining and using telephone and internet traffic data for criminal investigation and prosecution purposes. The providers are required to retain and secure the data, keep it available for criminal investigation purposes and to destroy it at the prescribed time. This process is regulated by the Radiocommunications Agency Netherlands (Agentschap Telecom). The Dutch Data Protection Authority has the more general task of regulating the use of privacy sensitive data. The Police and Public Prosecution Service use this data for the investigation and prosecution of serious crime, and the judiciary uses it in the legal decision-making process. This report focuses relatively sharply on how the stored data is used in practice, thus providing a clearer understanding of the usefulness and necessity of the retention obligation. How the Act works in practice is a complex issue, which is reflected in this report by describing how the various parties perform their tasks. This report provides fairly detailed information about how the stored data is used in practice. Other parties are touched upon, but do not form the main focus of this study.

Data collection

Various methods have been used to answer the research questions. As well as studying national and international professional literature, quantitative and qualitative information on the use of historical traffic data has been collected. Data has been collected from organisations such as the National Interception Unit of the national police, the Dutch National police, the judiciary (Public Prosecution Service) and the legal profession. A desk study was also carried out, which involved examining legal texts and their explanatory notes, secondary legislation, parliamentary papers, written documents of implementing agencies and scientific literature.

Seventeen face-to-face interviews and 16 telephone interviews were conducted for the study, which involved speaking to a total of 41 people in the period from June to October 2012. Additionally, court judgements were analysed to ascertain how the Dutch courts had used data kept available under the Act for criminal investigation purposes as evidence in criminal trials.

Remote communication, developments and implications

In recent years the mobile telephone has been replaced by the smartphone, and many people are online 24/7 these days. The use of smartphones means that people are much more likely to communicate in the form of short messages via apps and email, and phone calls are being made increasingly online as well.

Technological innovations and the accompanying fragmentation of communication and the use of various online services makes it difficult to keep track of all of a person's remote communication. Additionally, not all traffic data that is generated comes under the Act. Many internet users have email accounts with webmail services such as Hotmail, Gmail or Yahoo, which are provided by a foreign company. Consequently, the data is not necessarily retained for Dutch criminal investigation purposes. The same applies to providers of services in the *cloud*. In cases where investigative services none the less want to obtain traffic data from foreign suppliers they need to submit a request for legal assistance and have to wait and see whether the data is still available.

The legislative history and European regulations on the Data Retention Directive

Partly in response to the terrorist attacks in Madrid in 2004 and in London in 2005, 3 May 2006 saw the introduction of the EU Directive aimed at guaranteeing that certain telecom and internet data are retained and kept available for the investigation and prosecution of serious crime.

Retained data

Section 5 of the Directive stipulates the categories of data to be retained with regard to aspects including the designation, the date, the time and the duration of the communication. It is not permitted to retain data from which the content of the communication can be derived. The Member States were required to convert the Directive into national legislation by 15 September 2007; an extension was given until 15 March 2009 for the obligation to retain internet data. Not all the Member States have converted the directives into legislation. The term 'serious crime' has not been defined in the directives. This is reflected in the various grounds laid down in the legislation of the Member States that facilitate access to the retained data for criminal investigation and prosecution purposes. As with the duration of the retention period, the harmonisation envisaged by the EU legislation has only been achieved to a limited extent.

Privacy

The Act affects the privacy of members of the public. In the first place, the storage of telecommunication data involves a risk of unauthorised persons – such as hackers – gaining access to that data. A second, different type of breach takes place as soon as the police and judicial authorities are granted access to retained data in the context of an investigation. According to the ECHR it is permissible to limit the right to privacy only if provided for by law and necessary in a democratic society.

The Netherlands Penal Code stipulates who has access to the retained telecom and internet data and under which conditions. The Public Prosecutor can claim the issue of traffic data (Sections 126n and 126u of the Netherlands Penal Code) if there is a suspicion of an offence that merits pre-trial detention or a reasonable suspicion that crimes are being planned or committed in an organised context. An investigating officer can claim identifying data (Sections 126na, 126ua, of the Penal Code). The details that can be obtained are what are known as the user details (name, address, place of residence, number and type of service). If there are indications of a terrorist offence, the Public Prosecutor can obtain traffic data (Section 126zh of the Penal Code) and an investigating officer can claim user data (Section 126zi of the Penal Code). For an exploratory investigation into terrorist offences the Public Prosecutor can also claim databases of public and private bodies in order to have their details processed (Section 126hh of the Penal Code)

The retention and securing of the data in practice

The regulatory authorities

Compliance with the rules is supervised by the Radiocommunications Agency Netherlands, which operates as an independent regulatory authority and supervises compliance with the Act. The Radiocommunications Agency is a division of the Ministry of Economic Affairs and reports directly to the Minister of Economic Affairs. Additionally, the Dutch Data Protection Authority regulates all statutory regulations concerning the retention, use and processing of personal data.

The providers

Meetings were held with four providers in order to gain an understanding of how they approach the obligations under the Act. Prior to the retention obligation being introduced the retention periods varied between companies. Despite the Act's long start-up period, its implementation proved to be a sizeable project for the large providers.

At the two large suppliers interviewed for this investigation, a database is filled with data to be retained under the Act. This data is automatically destroyed when the retention period ends. A small provider interviewed for this study only recently actively started operating the retention periods because the quantity of data to be retained became too large. When they receive a request, the data applied for has to be taken manually out of the system by an employee.

The government has concluded an agreement with the large Dutch suppliers concerning remuneration for the personnel deployment needed to issue data retained under the various Acts and regulations to the government. Small providers are not covered by this arrangement.

The owners of a fourth interviewed supplier recognise themselves in the documentation of the Radiocommunications Agency as parties obliged to retain the traffic data of the email services they offer, but indicate that they do not comply with this for idealistic reasons. The researchers have asked the Radiocommunications Agency whether the services offered by this company are subject to the retention obligation. According to the Radiocommunications Agency they are not, but it acknowledges that certain parts of the legislation have become unclear owing to technological innovations.

Regulatory authority

The Radiocommunications Agency also oversees the implementation of operational processes. The supervision is provided for in a regulatory cycle in which the data suppliers are questioned about how they retain, secure and destroy the data. The Radiocommunications Agency does not however have the instruments and powers to regulate the content of the retained and delivered data. Section 18.7 (2) of the Dutch Telecommunications Act expressly stipulates that the regulatory authority is not authorised to retrieve traffic or location data retained by the providers under Section 13.2a of the Telecommunications Act.

The use of historical traffic data in practice

The Act makes a clear distinction between telephony and internet traffic data. To be perfectly clear, this report maintains that distinction. But in practice the distinction has virtually faded away and experts feel that the Act operates an incorrect division into two categories.

What is retained?

The annex to Section 13.2a of the Telecommunications Act contains a summary of the telephone data to be retained. This data includes the number of

the caller and the party called, the time and duration of the call and the location. This data must be kept for a period of 1 year. The content of a call or an SMS is not subject to the retention obligation. The traffic data of the sent or received message is subject to that obligation. Attempted calls in which no connection is made come under the retention obligation, too.

What is at stake

According to crime investigation professionals historical traffic data is retrieved in virtually all larger criminal investigations in which suspects or victims may have used their telephone. In 2012 the number of claims for the issue of telecommunication data totalled 56,825.

These claims were used to obtain information about the use of the telephone and possible IP-traffic, such as: the number that was used to make the call, when the call was made, the duration of the call and from which location, and whether there was any online contact. This information plays an important and highly valued role in criminal investigations. If an investigating team wants to obtain traffic data it has to obtain the approval of the Public Prosecutor. The investigating team has to indicate what it is seeking to achieve with the information, and obtaining the information must be proportional and observe the principal of subsidiarity. The intentions of the investigating teams in obtaining traffic data can be placed in a number of categories: (1) to identify a user, (2) to establish contacts, (3) to determine a location, (4) to trace an IMEI number, and (5) to make a decision on capacity before intercepting.

Relevance and retention period of telephony data

All of the interviewed professionals and experts said that they found historical data on telephone traffic to be highly relevant. A number of interviewed crime investigation professionals indicated that they wanted to obtain not only the start location (*first cell*) of a telephone call, but also the end location (*last cell*). However, the call ends, i.e. the final connection with a transmitter mast, is not stated in the annex to Section 13.2a of the Telecommunications Act.

It emerged from the interviews that most of the professionals and experts among the police felt that the one-year retention period is sufficient for the work that they do.

Historical internet traffic data

What is retained?

Historical traffic data concerning internet and email usage can yield information about matters such as the IP addresses someone has used, and the email contacts of the sender and receiver. The content of calls, messages or emails and search terms entered in a search engine and the IP addresses of searched internet pages are not covered by the retention obligation.

Relatively little deployment

It became clear during the interviews conducted for this study that the criminal investigation professionals had little or no knowledge of how historical data concerning internet traffic could be used for crime investigation purposes. Additionally, the work related to internet matters is often carried out by experts because the digitisation of today's society does not yet form part of the day-to-day work of many investigating officers. At the same time we established that technological developments move at a very fast pace. So fast that it is difficult even for the scarce experts to keep pace with them.

Historical internet traffic data is often retrieved in response to a crime or offence committed with the aid of or via the internet, such as sending threatening emails, internet fraud, human trafficking and the distribution of images of child sex abuse. The most important reason given for retrieving data is to *identify a user* or a connection. Fixed IP addresses usually remain unchanged for longer periods and the use can easily be traced either at the provider or at the Central Telecommunications Investigation Information Point. However identifying a mobile internet user on the basis of historical traffic data is a laborious process and in many cases not possible.

The relevance and retention period of internet data

According to various experts the majority of the internet data described in the annex to Section 13.2a of the Telecommunications Act is outdated. The regulation is no longer in keeping with today's internet usage or with the technological developments that have taken place in this area since the Telecommunications Act was introduced in 2009. This has led to the retention of data of members of the public that is not or is only barely used by the criminal investigation services. A meticulous review of the regulation governing IP traffic and the retention of IP data therefore appears appropriate.

The professionals and experts interviewed for this study and who are familiar with the internet traffic data all believe that the 6-month retention period is too short; there is clearly a need for IP traffic data that goes back further in time for criminal investigations into offences for which this data is retrieved.

The retrieval of transmission mast data

Retrieving traffic data based on a location yields information about all mobile telephones which, in the indicated time frame, have been called, have made calls or had an internet connection via the mast location in question. For permission to retrieve transmission mast data there must be a suspicion of an offence as specified in Section 67 (1) of the Netherlands Penal Code and the use of the data must be in the interest of the investigation.

Transmission mast data is retrieved mainly for serial offences. In such cases the data of various locations is compared with the aim of pinpointing a recurring number. Of course, this detection method only has a chance of success if the suspect used his telephone around the time of the offence.

Alternative?

Opponents of the retention obligation regard the targeted freezing of data as being a less privacy-violating solution because this involves a specific data set that is retained for longer rather than retaining all the data of all of a provider's customers. None of the experts we spoke to felt that freezing data was a comparable or equivalent alternative to a general retention obligation because this would rule out the possibility of retrieving data retained a longer time ago. To be able to use this data it is necessary to know in advance – when the data is still available and can be frozen – what data will be needed at a later date. Given that it is sometimes not until later that offences come to the knowledge of the police, and suspects are sometimes not identified until long after a crime has been committed, it is necessary to retain this data for later use in the criminal investigation process.

The use of traffic data in figures

The Telecommunications Act makes it compulsory to publish the number of enquiries about telecommunications traffic made by criminal investigation services each year (Section 13.4 (4) of the Telecommunications Act. In 2012 a total of 56,825 claims for the issue of traffic data were made. However the number of claims announced by the Minister also includes data not covered by the Telecommunications Data (Retention Obligation) Act.

It should also be noted that the retrieval of telecom data in the Netherlands is registered by telephone number, IMEI number, IP address or 'mast location' on which data is retrieved. These figures do not provide an insight into the number of people whose telecommunication data is retrieved each year, or the number of criminal investigations or the nature of the investigations for which the data was retrieved. Neither do the figures provide any insight into the extent to which a claim has actually resulted in data being issued.

Court judgements

This report also provides an insight into the use and value of traffic data in court judgements. A total of 74 rulings were found between July 2012 and February 2013 in which the term historical traffic data concerning telephony occurred. This data was generally used in the rulings to demonstrate 'contact between suspects' and 'locations'.

A search for cases in which IP traffic data was used in the judgement revealed 26 judgements in the period from January 2009 to February 2013. This IP data was mentioned mainly in the rulings on criminal investigations into images of child sex abuse. More than half of the judgements concerned the downloading and/or distribution of images of child sex abuse. The retrieval of this data is not so much about where the suspect was and with whom he communicated, but sooner whether the suspect can be linked to the internet address that was used or other user data.