Evidence for necessity of data retention in the EU

Table of Contents

1. Introduction

This document draws together evidence which has been supplied by Member States and Europol in order to demonstrate the value to criminal investigation and prosecution of communications data retained under the Directive 2006/24/EC (the Data Retention Directive or 'DRD'). It contains some general context on the role of historical data in various types of investigations, some observations on the available statistics, and a selection of individual case studies which have been provided by Member States. It is intended to provide further information on the question of the necessity of data retention; readers should also consult the evaluation report for the Commission's general evaluation of the DRD,[1] which included (section 5.4) a number of the arguments which are developed in this document, along with a few illustrative examples, and other statements including replies to questions from the European Parliament[2] concerning the role of communications data in the investigation and prosecution of the most serious crimes.

2. Context

Crime in the EU[3] is increasingly characterised by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by widespread illicit use of the internet. These groups focus their activities where they perceive the risks of detection to be low, like credit fraud and counterfeiting, which along with trafficking in weapons, drugs and human beings are also extensively used to finance terrorist activities. The EU furthermore is a key target for cybercrime, and the prevalence of internet technology has created a market for child abuse material.

Criminal exploitation of communications technologies mirrors general trends in consumer behaviour. In the 1990s a typical user might make 10-20 fixed line or mobile calls a day and send two or three SMS over a few networks; in the 2000s with increased volume and network coverage, a typical user might make 15-25 calls and send 5-15 emails and SMS, and also use online chat, browsing and 'voice over the internet' services.[4] Internet protocol (IP) traffic volumes were estimated to have more than trebled between 2007 and 2010,[5] and in the current decade the internet is the primary source of communication.

Criminals attempt to evade detection through the use of false identities or anonymous communications services. Investigators therefore need not only to be able to access traffic and location data and associated identification details, but also to be confident that these data cannot be fabricated or falsified. The access by and exchange between law enforcement authorities of these communications data is essential to the successful disruption of organised criminal networks.

---

[1] COM(2011)225, 'Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)' http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

[2] E.g. E-004636/2012

[3] See Commission Communication 'First Annual Report on the implementation of the EU Internal Security Strategy', COM(2011) 790 Internal Security Report; Europol: Organised Crime Threat Assessment (OCTA) 2011.

[4] Analysys Mason, Europe's Digital Deficit: Revitalising the Market in Electronic Communications, 3 March 2010.

[5] Source: Cisco Visual Networking Index.

Communications data which do not concern the 'content' (e.g. the conversation during the telephone call, the message in the email) but rather the 'envelope' or 'metadata', consist of information on the identity of subscribers or clients (i.e. service-associated information e.g. IP addresses), traffic data (i.e. communication-associated information e.g. logs of calls received and made), and data on the location of the user at the time of the communication.[6] Such non-content data were used before the adoption of the DRD in high-profile investigations including the murder of Irish journalist Veronica Guerin in 1996, the uncovering of a massive international drug trafficking ring centred around the 'Ndrangheta mafia organisation (known as operation IBISCO), the murder in 1998 of Corsican police prefect Claude Erignac, and the 2004 Madrid bombings.

The DRD was adopted on 15 March 2006 with the aim of ensuring that such data be retained for between six months and two years and be available for the purpose of the investigation, detection and prosecution of serious crime. It is in force in most Member States.[7] The Commission's evaluation report, published in April 2011,[8] concluded that, given the objectives of the Internal Security Strategy[9] and the Digital Agenda,[10] the EU should continue to support and regulate the storage of, access to and use of communications data, but should improve EU rules to prevent the different types of operators facing unfair obstacles in the Internal Market and to ensure that high levels of respect for privacy and the protection of personal data are applied consistently.

3. How communications data are used

During criminal investigations requests for communications data usually proceed - and often result in – the arrest of suspects, bringing of charges or the exclusion of people from investigation. Fewer data are used during prosecution proceedings in court. This may be because prosecuting authorities are unlikely to use information about individuals who have been investigated and then deemed to be of no further interest to the investigation, or because accused parties when confronted with evidence provided through communications data decide to enter guilty pleas which thus remove the need for the communications evidence to be adduced in court. Communications data are used to corroborate other evidence like witness statements and evidence of the association of suspects and location and chronology of event. Some crimes may be dealt with through administrative means (e.g. a caution), and certain investigations may be unable to progress for various reasons. Consequently, more data tend to be acquired initially by the investigator than is later relied on in court. Defence counsel also obtain access to these data: one UK authority reported that there had been 204 such requests between April 2009 and March 2010.

---

[6] These types of data are reflected in Article 5(1) of the DRD i.e. from whom (sub-article a)) and to whom (b) the communication was sent, when it was sent and how long it lasted (c), what sort of communication (d), how the communication was sent i.e. what equipment was used (e) and where the communication was sent (f). For definitions see ETSI Technical Standard 101 331.

[7] The deadline for transposition was September 2007, with the option of postponing the implementation of retention of internet data until March 2009. Twenty-six Member States have transposed it, two (Belgium and Germany) have partially transposed it.

[8] COM(2011)225, 'Evaluation Report on the data retention directive (Directive 2006/24/EC)'

[9] Commission Communication, 'The Internal security strategy in action: Five steps towards a more secure Europe,' COM(2010) 673.

[10] Digital Agenda, COM(2010) 245 final/2.

4. Overview of types of cases in which data are important

The importance of subscriber, traffic and location data is demonstrated by research and the practical experience in the EU. Since the adoption of data retention measures, Member States as well as Europol have provided a considerable number of case studies in which data have proven important or crucial in solving some of the most serious crimes. These data can be the only lead to identify a suspect or to identify his/her accomplices at the start of an investigation where eye witness accounts or confessions and other forensic evidence are unavailable, and to decide whether it is justified to use more intrusive surveillance tools like interception. They can help establish whether an offence was planned in advance. They are particularly valuable for cases where internet/communication services are used to commit a crime, such as grooming and uploading/downloading child pornography and identity theft: for example, where someone is detected in an internet chat room attempting to sell child pornography, investigators need first to find the IP address used to connect to the chat room, and then ask the internet service provider (ISP) to identify which individual user has been assigned that particular IP address. Similarly, where threats to commit suicide or attack others are placed on the internet (e.g. Sweden claims to have investigated 15 such threats to carry out massacres in schools over 12 months in 2009-10), police can only begin investigation through identifying the user of a particular IP address based on data held by the ISP.

While most data tends to be requested within a few months or even weeks of the communication taking place, there are four categories of criminal investigation for which **older data** tend to be needed.[11]

a. **Terrorism and organised crime** including severe types of financial crime which are often characterised by repetition or by a long period of preparation. Investigations often require time in order to establish a clear pattern and relationships between multiple events and so to expose not just individual suspects but whole criminal networks, especially where associates repeatedly exchange SIM cards to avoid detection. The gap between the moment the criminal offence is committed and the moment of its detection by law enforcement authorities, through the identification and seizure of servers containing evidence, can be several months or even years. Such delays occur in cases of:

   i. trafficking in human beings and drugs trafficking, where there is a complex division of labour among accomplices;[12]

   ii. repeated extortion where victims are in a relationship with the offender and where the victim may only seek help months or even years after the exploitation started;

   iii. tax fraud, serious cases of financial crime and corruption of public officials which may span several years. Such offences may only be detected after the end of a financial year, after audits have been carried out or on the basis of annual reports. Authorities may therefore need to examine data which are at

[11] See the Commission's evaluation report.

[12] Prosecutors in Poland study traffic data in 70% of preparatory proceedings in drugs possession cases. E.Kuźmicz, Z. Mielecka-Kubień, D. Wiszejko-Wierzicka (red.) Karanie za posiadanie. Artykuł 62 ustawy o przeciwdziałaniu narkomanii – koszty, czas, opinio. Raport z badań, Instytut Spraw Publicznych, Warsaw 2009, s.58.

least a year old, or several years old to investigate 'triangulation' structures involving false invoices or transactions which appear at first to be legal, especially across jurisdictions;

iv. repeat burglaries, where proof of involvement of the same gang often depends on mobile telephone location data which shows connected individuals to have been in the same area at suspicious times of day.

b. **Serious sexual offences** where the victim may not report the crime for months after the event. UK report that over half of communications data used in such investigations were six months old or over.

c. **Substantiating previous intent to commit illegal activities**, which is important within criminal and pre-criminal proceedings and to determine whether a homicide is a case of premeditated murder;

d. **Large cross-border cases** which may involve mutual legal assistance procedures, such as offences committed by travelling gangs or where several requests for data from different operators are often necessary. It is often only after months of investigation that all relevant facts are collated. Where servers are located in a foreign country data logs held on servers must be analysed to extract the IP addresses of computers used by persons suspected of accessing the child abuse images. Shorter data retention periods often make it impossible to obtain effective results. Rogatory letters take time to execute, and as a result IP addresses and telephone numbers may be identified for which subscriber data can no longer be requested.

5. Consequences of absence of data retention

The crucial value of mandatory communications data retention as a measure, as distinct from communications data *per se*, is the *guarantee* that potentially valuable data will be available for a given amount of time. Other measures, such as rules on data preservation (or 'quick freeze'), whilst valuable in many ways, signally fail to provide such a guarantee, and as such rely wholly on the need or willingness of operators to store these data for their own commercial purposes, and to do so in such a way as to render these data accessible in time to be valuable to investigations and prosecution. Before the DRD entered into force, operators may have stored some data but not in an easily retrievable way: mobile telephony data might have been stored in a street-side cabinet or mobile telephone tower, while ISPs may not have logged IP addresses in many cases where they are switched frequently (in processes known as dynamic address allocation and load-balancing). However, according to data protection authorities and operators, certain data have minimal business value and are only stored in a retrievable form because of mandatory data retention. Such data include: (a) fixed/ mobile traffic data for flat-rate unlimited use contracts and pre-paid services;[13] (b) source ID (i.e. telephone number) for incoming calls; (c) unsuccessful call attempts; (d) IP addresses[14]; (e) cell ID (i.e. location) data; and (f) email data. The absence of a guarantee of the availability of

[13] In Germany, the proportion of private internet users with such flat-rate plans rose from 18% in 2005 to 87% in 2009. The proportion of users of prepaid services varies, from about 20% in Finland to about 80% in Portugal. Some Member States (Bulgaria, Denmark, Greece, Italy, Slovakia and Spain) require registration of all pre-paid SIM cards, though there is no evidence of the efficacy of this as a law enforcement measure.

[14] This will change with when the Internet Protocol version 6 is deployed, that is the so-called 'internet of things' where virtually any object could be integrated into the information network with a unique IP address.

these data is deemed to constitute an unacceptably high risk to the ability of police and judicial authorities to investigate and prosecute serious crime, particularly in cross border cases.

If certain traffic data were not stored, detecting and investigating certain crimes would be practically impossible. The experience of Germany since the constitutional court judgment annulling data retention measures in March 2010 may illustrate the consequences of the absence of mandatory data retention. According to the German federal police (*Bundeskriminalamt*) and state police (*Landeskriminalämter*),[15] for 44.5% of the cases involving requests for historical data traffic data, there was no other means of conducting the investigation. They reported that 30% of criminal cases have collapsed since the judgment of the Constitutional Court.[16] According to the Lower Saxony *Landeskriminalamt*, between the judgement of the Constitutional Court and summer 2011, traffic data would have been requested had they been available; in 257 cases (or 75% of all cases) investigations could not be solved, while for 32 cases (9%) investigations were only solved by investing significant additional resources. These claims should be considered in the light of a report completed in July 2011 and published in January 2012 by the Federal Minister of Justice, which concludes that the present situation is characterised by very limited statistical and empirical data.[17] Meanwhile, according to the statistics provided by Czech Republic, the number of unsuccessful requests for data increased from 3% in 2009 to 14% in 2011, the year in which the constitutional court annulled the legislation transposing data retention.

6. Cross-border aspects of data retention

Member States regularly exchange requests, with a copy sent to Europol, for investigations of serious crime, with an estimated 50% (or 40 000) of these requests involving communications data.[18] The exchange of traffic or location data requires mutual legal assistance procedures which, according to law enforcement authorities, can be slow and result in delays in investigations and the loss of associated data if the target of an investigation switches SIM cards or IP addresses while the request is being processed. Where there is a good level of trust (e.g. Franco-Spanish cooperation against the ETA terrorist threat) it seems that data are exchanged more easily. One UK law enforcement authority over a six month period in 2009-10 reported five operations which required communications data and which resulted 14 cases brought before courts in another Member State or outside the EU, each of which resulted in a conviction. Lithuania in its statistics for 2010 reported that, of the total of around 136 000 cases in which data were requested in 2010, 23 000 concerned requests for legal assistance from other Member States in relation to high-volume and high-value mobile telephone theft.

---

[15] Sachstandsbericht Nr. 8: Stand der statistischen Datenerhebung im BKA, 23 June 2011, at 13.

[16] http://www.faz.net/artikel/C30833/straftaten-im-internet-lka-direktor-jeder-muss-identifizierbar-sein-30334057.html

[17] Max-Planck-Institut für ausländisches und internationales Strafrecht: *Schützlücken durch Wegfall der Vorratdatenspeicherung: Eine Untersuchen zu Problemen der Gefahrenabwehr und Strafverfolgen bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, July 2011.

[18] Source: Workshop with police on future options for data retention in the EU, 17 June 2011. 'Serious crime' is defined in Council Decision 2009/371/JHA establishing the European Police Office (Europol).

7. Statistics and quantitative data

Article 10

Article 10 of the DRD requires Member States to provide the Commission with statistics on a yearly basis which should include:

- the cases in which information was provided to the competent authorities in accordance with national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

In November 2008 the Commission expert group on data retention[19] adopted a template for submitting these statistics, which was presented to Member States delegations at a meeting in January 2009. The delegations undertook to provide annual statistics on the basis of that template.

Available statistics

Twenty-three Member States have provided some statistics since 2008. While most Member States have used the 2009 template, they interpret in different ways terms from the DRD such as 'case' and 'request', and statistics vary in format which limits their comparability. (Poland's statistics alone account for around half of requests reported overall, partly because competent authorities submit identical requests to each of the main mobile telephone operators.) It appears that there are over two million requests per year for retained data, equivalent to about two requests for every police officer in the EU or 11 requests for every 100 recorded crimes. The number of requests varies greatly between Member States. Certain Member States (France, Poland and UK) claim that communications data are needed for most criminal investigations. UK claims that for an 'average' murder investigation, there may be between 500 and 1000 communications data requests.[20] Finland stated that 56% of all requests for data proved important or essential to the outcome of criminal investigation or prosecution. Each investigation into a serious crime is likely to require multiple items of data. UK reported that for a certain investigation 120 applications were made, including 17 for traffic data, 45 for 'service use data' and 58 for subscriber data, resulting in nine convictions.

Most requests concern mobile telephony data (approximately 75%). Approximately 67% of data is requested within three months and 89% within six months, but a sizeable minority of requests – 11% - concern data 6-12 months old. Ensuring that data are retained for more than six months helps prevent investigators from asking for excessive amounts of untargeted data earlier on in the inquiry.

---

[19] See http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/index_en.htm

[20] Home Office in oral evidence to Joint Committee on Draft Communications Data Bill, UK Parliament, 10 July 2012.

Limitations of quantitative data

The Commission considers statistics on crime and criminal justice to be indispensable tools for developing evidence-based policy at EU level, and continues to work to address the general lack of comparable statistical information.[21] Certain NGOs have attempted, using selected crime statistics, to draw negative conclusions about the value of data retention.[22] These claims fail to acknowledge that crime statistics – including the number of crimes and the number of crimes which are solved ('clearances') - are determined by multiple socio-economic factors, and success in tackling crime cannot be attributed to a specific security measure, such as data retention.[23] Police use different methods for measuring crime clearance rates and, moreover, it may be argued that an undue focus on such statistics can be counterproductive to the effectiveness of law enforcement.[24] In any case, it would not be possible to identify meaningful statistical trends only a few years after the DRD entered into force.

Conceptual and methodological issues

A number of areas of confusion regarding Article 10 remain.

a. There are different interpretations of the term 'cases' – which could mean (i) each and every item of data that was or was not provided, (ii) each request which may be for one or multiple sets of data, or (iii) each investigation in which there might be multiple requests for multiple items of data.

b. Where the request to a service provider is for more than one item of data, the data may be of different ages. Recording the age of individual data records could be unduly onerous for operators and/or competent authorities.

c. Statistics submitted from some Member States only refer to requests for traffic and location data and not to subscriber information acquired from operators.

d. The phrase 'Cases where requests for data could not be met' has been interpreted variously as cases where i) the service provider was unable to provide data that should have been retained under the DRD but were not retained; ii) data that were needed but which do not fall within the scope of the DRD, or iii) data that had been retained but were no longer available because the request was made after the expiry of the retention period.

---

[21] See COM(2012) 713, 'Measuring Crime in the EU: Statistics Action Plan 2011- 2015'.

[22] See, for example, http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[23] See K. von Lampe, 'Measuring organised crime: A Critique of current approaches', in *Threats and Phantoms and Organised Crime, Corruption and Terrorism*, eds. P.C. van Duyne, M. Jager, K. von Lampe and J. L. Newell, 2004, pp. 85-110.

[24] See for example J.H. Skolnick and D. Bailey, *The New Blue Line: Police Innovation in Six American Cities*, New York, 1986: 'Variations in crime and clearance rates are best predicted by social conditions such as income, unemployment, population, income distribution and social heterogeneity'.

The expert group addressed this issue and in November 2012 adopted updated and more comprehensive guidance on provision of statistics under Article 10, which the Commission encourages all Member States to follow.[25]

Furthermore, Member States law enforcement authorities and data protection authorities are generally not in a position to know whether the precise data used in investigations and prosecutions was stored by the operators solely in order to comply with the data retention obligation. There is no obligation to store separately those data needed for (a) business purposes), (b) purposes of combating 'serious crime', as referred to in the DRD, and (c) for public order purposes other than combating serious crime, which may be permitted under Directive 2002/58/EC. Supervisory authorities do not have enforcement powers to ascertain which data is kept for which purposes, although, according to a report by the Article 29 Working Party, separation seems to be the norm in most Member States.[26]

8. Qualitative data

Member States are under no obligation to provide evidence of the value to serious criminal investigation and prosecution of *retained data* (i.e. data kept only because of mandatory retention). The Commission nevertheless wrote to each Member State in February 2012 with some specific guidance – consistent with the deliberations of the expert group - on qualitative and quantitative evidence to be provided. The evidence in this document includes responses to this request, as well as other examples provided before and since the publication of the evaluation report. Below are case studies provided by Member States in order to illustrate the importance of historical data; some of these cases predate transposition of the DRD in the Member State in question. Some cases may be understood as 'negative' examples – that is, examples of where investigations have stalled because of the absence of a data retention requirement. Some examples are more elaborated than others.

Terrorism

Case 1 (Germany)

Individuals were suspected of supporting Al-Qaida and the Uzbekistan Islamist Movement by distributing propaganda material on the internet and trying to attract supporters for their cause. The internet access provider had not retained the IP address of one user who had logged in to establish an internet video channel for those purposes, and investigators were unable to pursue that part of the inquiry.

---

[25] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/docs/guidance_on_statistics_position_paper_16_datret_final_en.pdf

[26] Article 15(1) of Directive 2002/58/EC on 'e-Privacy' allows Member States to restrict privacy rights and obligations, including through the retention of data for a limited period, to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. See EDPS opinion on evaluation report on the DRD, May 2011 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf and Article 29 Working Party Report 01/2010 'Report 01/2010 on the second joint enforcement action: compliance at national level of telecom providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of article 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/E amending the e-Privacy Directive' http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf. Recital 12 of the DRD acknowledges that data may be retained beyond the categories in the scope of the DRD and for purposes other than those set down in DRD.

Case 2 (Germany)

In an internet forum on 12 April 2010 a video of a terrorist organisation was made available through various internet links. One of these links had been created by an unknown person registered under a certain e-mail address. An inquiry concerning the e-mail address with the responsible email service provider revealed that it had been registered only a day before the release of the video. The IP address had been allocated by a major ISP, but as seven days had already elapsed the ISP said they it did not hold the IP address details. The person could not be identified and the case remains open.

Case 3 (Germany)

Following the murder of Hamas official Mahmoud al-Mabhouh in Dubai 2010, an investigation was conducted into a person suspected of acting an agent for an intelligence service and of misleading another to make false official entries. Financial investigations revealed that calls made via one of the suspect's mobile telephone were billed retrospectively over a period of four to six months. It is likely that analysis of communications data contacts would have enabled the identification of further leads and collaborators in Germany. However the communications data were no longer stored. Consequently, it has not been possible to date to progress the investigation.

Case 4 (Germany)

Information was received by US and Lebanese authorities on attacks in Germany in 2010 planned by members of Fatah al-Islam. This led to preventive measures with the aim of identifying possible cell members in Germany and communication among them. In the end, only one of the persons mentioned was identified in Germany. This person, who had been staying in Germany under a false identity, was also the subject of an arrest warrant issued by the Lebanese authorities for general offences. This person has been arrested and is being detained pending extradition. The suspicion that this person posed a terrorist threat has been eliminated. All additional measures taken against the group were fruitless since the historical communications data were not fully made available by the providers.

Case 5 (UK)

Operation Vivace, an investigation into four attempted bombings in the London area on 21 July 2005 which mirrored those carried out a fortnight earlier on 7 July, made extensive use of historical communications data. These data identified regular contact between the main five offenders and assisted in identifying further offenders who were arrested and charged with offences relating to the attacks. The data placed some the offenders close to the attack scenes prior to and after the attempted attacks on 21 July, and routinely placed four of the offenders in the vicinity of the bomb factory, showing that three of the defendants were there the night before the attacks. The data also implicated two suspects who provided material assistance to offenders during their escape after the attacks from London to the south of England and then abroad. These investigations lasted between several months and several years, with fresh information coming to light throughout the process. As more information was gathered, so further fresh target communications were identified. Equally, as each day passed, historical communications data was lost as it was deleted from operators' storage databases in line with data retention policy along with potentially valuable leads.

Murder and manslaughter

Case 1 (Czech Republic)

Czech investigators suspected that prior to a murder committed in the Kroměříž region in June 2011 the victim and accomplice had been close acquaintances. Communications data were requested immediately but operators stated that in order to comply with the national constitutional court judgment the data had been deleted. Authorities needed over a week to assemble other biological evidence and witness statements before they were able to secure the suspects arrest, whereas communications data could have been expected to provide grounds for arrest on the day of the murder and so avoid risk of further danger to the public.[27]

Case 2(Czech Republic)

During investigation into a murder committed in September 2011 police were unable to assemble sufficient evidence due to the unreliability of witness statements. Police were aware of the mobile telephone numbers that were used by these persons and whose devices were probably switched on at the time of murder. However service providers were no longer keeping the data necessary to identify the location of mobile communication equipment. A lot of interrogation has been carried out by police along with other operations but without any results. Police consider that had they been able to access these data they would have identified the perpetrator.

Case 3 (Czech Republic)

A Roma dwelling in Vítkov was subject to an arson attack in 2009. The court classified the conduct as an attempted multiple racially-motivated homicide. At the scene of crime there was no clear evidence leading to the perpetrators. Police investigation led to the information that an individual, 'J.L.', had been heard telling people in a nightclub about plans to 'go after gypsies'. J.L. was known to be a right-wing extremist who had taken part in a number of public gatherings. Analysis of his mobile telephone revealed connections to one suspect who shortly after the attack was known to have burns on his arms, and data related to his mobile telephone in turn enabled police to identify further perpetrators.

Case 4 (Denmark)

An elderly woman was discovered dead in her home. Subsequently 6000 DKK (800 EUR) worth of transactions were made using her bank card. Police studied CCTV footage from locations where the card was used, and images were released to the press but there were no positive identifications of any suspect. Communications data obtained following a court order enabled investigators to identify mobile phones which were within the vicinity of the credit card transactions and at the estimated time of death of the woman. A young male was at first suspected but later was excluded as he had not been in the areas where the card was used. Investigators then identified two brothers using the call data, leading to their arrest.

---

[27] http://www.novinky.cz/krimi/236446-muz-obvineny-z-brutalni-vrazdy-studentky-v-huline-tvrdi-ze-se-zabila-sama.html

Case 5 (Denmark)

A 33-year-old man was shot dead in a rural area where he regularly went fishing with his partner. His female partner who was near the scene at the time was suspected by investigators of involvement in the murder, which she denied. Police obtained a warrant to carry out wiretap and obtain historical communications data concerning the partner. These data revealed that the partner had been in contact with a male by telephone calls and text messages during the hour leading up to the murder. Police then obtained communications data associated with this person, leading to the arrest of both individuals. Location data was used to refute the man's alibi that he had been at his home 25 miles away from the murder scene, and he subsequently confessed to murder and implicated the woman in the conspiracy. Each of them was sentenced to 13 years' imprisonment for manslaughter.

Case 6 (Denmark)

An investigation into six attempted murders, assault and the possession of a stash of weapons in connection with wars between biker gangs involved analysis of over 730 000 items of historical call data associated with around 85 telephone numbers. These data supplied evidence which corroborated the statements of key witnesses and culminated in the conviction in September 2011 of 15 gang members and sentences of a total of 135 years' imprisonment.

Case 7 (Germany)

Polish authorities were searching for a murder suspect, believed to be in Germany, who was known to log on regularly to a Polish social network. Polish authorities sent to German authorities a list of the login data including the IP addresses, which were their only lead. All these data had been deleted by the ISP in Germany, and the case remains open.

Case 8 (Germany)

After the murder of a police officer the offender escaped in the car of the victim. The examination of the scene of crime did not yield any additional information on the identity of the offender. No eye-witnesses were known. Investigators had reason to believe that the offender had abandoned his vehicle and had made a call to a taxi firm using a mobile telephone. The network provider had deleted all traffic data, which might have enabled police to identify the offender.

Case 9 (Germany)

A body found in a street in Cologne was identified several days later as a 43-year-old Italian national. The Italian authorities advised that the victim was believed to have been connected with the mafia. It took three months of investigation to identify the possible scene of the murder and three suspects. By this time historical data relating to the suspects' communications and location were not available, and the investigation is still unresolved.

Case 10 (Estonia)

Sergey Kulešov was convicted in 2009 for murdering his female business partner in 2006 on the basis of traffic and location data of mobile telephone communications which connected him with the victim and the scene of the murder. There was no other clear evidence other than suspected motivation which emerged during the investigation.

Case 11 (Hungary)

An investigation in 2009 was opened into a homicide involving an unidentified individual who was believed to have unlawfully entered a privately-owned farm with the intention of committing burglary. The suspect killed the victim by striking him several times on the head with an axe found at the scene of the crime. He stole cash and valuables worth about 270 000 Forints (1000 EUR). He hid the victim's corpse in a cesspit in the grounds of the farm. Location data retained by the service provider enabled investigators to connect the suspect with the scene and time of the homicide and then to a location 200 kilometres away from the farm where the suspect was tracked down and arrested.

Case 12 (Luxembourg)

In 2011 a body was discovered in a forest hanging from tree. There were no identification documents and the state of decomposition of the corpse suggested it had been left for several weeks if not months. Investigators had been unable to identify the body. Around 10 months after the unidentified person's death, contacts outside Luxembourg led to a suspicion that the death may have been the result of a criminal offence rather than suicide. By this point, however, it communications data which may have enabled a reconstruction of last movements and communications of the person were unavailable.

Case 13 (Luxembourg)

A man was suspected of conspiring with his partner of murdering his adoptive parent. The investigating judge ordered disclosure of traffic data dating back over three months concerning these persons' telephone activities. These data enabled investigators to link the suspects to the contract killer and to refute the stories of several credible witness statements to the contrary.

Case 14 (Luxembourg)

In August 2008 a man's body was discovered abandoned in a forest. The investigating judge ordered disclosure of communications data relating to telephone calls made by the victim's wife several months prior to the murder. These data enabled investigators to identify a suspect who confessed to the murder and to the fact that it had been contracted by the wife since early 2007.

Case 15 (Netherlands)

A man was shot dead in the basement of his electronics stop in Rotterdam in September 1999. His wife was suspected of complicity in the murder but the prosecution initially failed due to lack of evidence. Subsequently, using traffic and location data investigators were able to link the woman to the man who carried out the murder, and Rotterdam District Court sentenced her to 12 years imprisonment in July 2010.

Case 16 (Poland)

In February 2007 in Myślenice two owners of a currency exchange office were shot dead with machine guns. The perpetrators stole 150 000 PLN (37 000 EUR). Investigators obtained communications data which enabled police to arrest the suspects three weeks after the murders had taken place. Analysis of the calls made using the suspect's SIM card which had been seized enabled investigators to implicate the suspects of the February 2007 murders in

separate similar murder case. Further investigation led to three individuals being charged and in July 2010 convicted by the District Court in Kraków on three counts of murder and two of attempted murder between 2005 and 2007 in Kraśnik, Tarnów and Sosnowiec. Tadeusz G and Wojciech W were sentenced to life imprisonment and Jacek P to 15 years imprisonment.

Case 17 (Slovakia)

On 22 June 2011 a man was lured from a 'casino-café' in Bratislava to nearby Vráble and killed with eight gunshot wounds in his own vehicle, before being driven and his body disposed of in Jabloňovce. Communications data provided investigators with evidence that the murder had been premeditated. The accused was believed to have telephoned an accomplice the day prior to the murder to arrange transport. Location and call data implicated the accused at the murder scene, corroborating the statements of witnesses that he had made telephone calls on arrival at and departure from the location. Together with the conclusions of the forensic autopsy, the data helped establish that the victim was dead by the time the perpetrator left the scene of the crime. During the court proceedings, these data made it possible to refute the perpetrator's defence as to the sequence of events, and contributed significantly in establishing that the perpetrator had planned and prepared the murder of the victim in advance. (To this end, he had already dug a hole, in which he subsequently buried the victim's body within 30 minutes of inflicting the fatal stab wounds.) These findings ultimately resulted in a change in the legal classification of the crime to a more serious offence with the prospect of a more stringent penalty.

Case 18 (Slovenia)

Italian police alerted authorities in Slovenia, Croatia and Bosnia and Herzegovina following the disappearance of Roberto Menicali in June 2011 who was believed to have crossed the Italy-Slovenia border with the intention of selling his car to a man and a woman. Authorities were able to connect movements of the missing person's car, use of his bank card and traffic data from mobile phones and thereby to establish that the suspects were citizens of Bosnia and Herzegovina. Analysis of data from Menicali's mobile led police to the discovery of a man's body in woods near Nova Gorica, later established to be that of Menicali's, and subsequent cross-border cooperation with authorities of Serbia and Montenegro resulted in an international search warrant and the arrest of both suspects in Montenegro.

Case 19 (Sweden)

In July 2010 police began an investigation into a series of shootings, the first of which occurred in October 2009 and involved the death of a young woman and the serious injury of a young man. Investigators obtained traffic data from the crime scene to identify possible suspects. Analysis of these data along with a psychological profile led to the suspicion of a single individual using a legally-obtained weapon. The police received a tip-off and the person was arrested. Ballistic evidence connected him to some of the shootings. In order to connect him to all the shootings and to rule out other possible suspects the investigators used traffic data, some of which was over 10 months old, from mobile telephone operators as well as information from banks and other sources which revealed the suspect's movements.

Case 20 (Sweden)

Anders Eklund was convicted in 2008 for the murder of 10-year-old Engla Hoglund. There was a reasonable assumption that Eklund could have committed other crimes that were not

known to the police, and these suspicions were substantiated by location data generated by his mobile telephone along with other evidence such as DNA analysis, leading to the conviction of Eklund for the murder of Pernilla Hellgren in Falun in 2000.

Case 21 (UK)

In September 2009 the body of taxi driver Stuart Ludlam was discovered with two gunshot wounds to the head in the boot of his taxi outside the train station in Derbyshire. Police carried out checks on the mobiles Ludlam was carrying at the time of his murder in order to help identify his killer. His work telephone had been stolen but data on communications using that device were identified through subscriber checks which revealed that Ludlam had received diverted calls from the main taxi office number. Incoming and outgoing call data with cell site locations were requested to trace Ludlam's movements on that day. Call data was of no use at this time as it only showed the taxi number on divert calling. Police then applied for call data for the taxi landline number to identify the last number to have contacted Ludlam and any other numbers that might be of interest to the investigation, in order to establish how he might have been lured to the murder scene. The last number to have called the taxi company was attributed to a pre-paid SIM card for which there were no subscriber details. Using the telephone data police were able to identify the place where the telephone had been purchased and where the last top-up before the murder had been purchased, which was at a supermarket petrol station a few days beforehand. The petrol station did not have in-store CCTV but police requested the till records which revealed another transaction of 20 GBP of petrol at the same time as the purchasing of the mobile telephone top-up. Officers now knew the time the top-up was purchased, and so examined all CCTV tapes from locations in the vicinity of the supermarket, which showed a male purchasing a mobile telephone in a nearby shop. This male was identified as Colin Cheetham, who after further investigation was convicted of Ludlam's murder and jailed for 30 years. Without access to relevant traffic data Cheetham might never have been identified.

Serious sexual offences and child abuse

Case 1 (Belgium)

A Belgian lifestyle and relationships website (zoetie.be) hosts a forum in which teenagers exchange questions and answers. An 11-year-old girl was groomed by someone pretending to be a 17-year-old male who attempted to persuade her to have sexual intercourse with an older man in exchange for money and designer clothes. The girl's father discovered these exchanges and informed the police just before the girl and the boy had arranged to meet. Following three-months of investigation, including the use of IP addresses and assistance from communications service providers which had set up the e-mail addresses used to contact the girl, police identified their suspect as a 35-year-old man. Investigators needed to build up evidence from computers seized from at the man's house, from data obtained via letters rogatory from a communications service provider based in the US. Ten months later the offender was given a suspended sentence and ordered to pay substantial damages.

Case 2 (Czech Republic)

In Olomouc region, a girl under the age of 15 was coerced into prostitution by a man through a social media channel. The man arranged for her to have sex with 10 men over nine days in January 2012. He was identified by traffic data generated by his interaction with the girl and subsequently charged with trafficking in human beings and sexual abuse.

Case 3 (Czech Republic)

In 2011 police investigated the operator of a pornography website which announced the availability of child pornographic images. Internet data enabled investigators to locate the computer from which images had been uploaded, and led to the charging of two persons for sexual abuse of a seven-year-old girl and production of child pornography.

Case 4 (Europol/UK)

In 2007 UK and Australian authorities independently discovered boylover.net, a covert forum for adults to discuss their sexual interest in young boys. Subscribers to the forum once they had made contact with one another would then move to more private means such as email to exchange and share images of children being abused. Police detected 70 000 such subscribers across the UK, US, New Zealand, Australia and Thailand.

As a result Operation Rescue was launched, in which Member States authorities monitored the internet and obtained relevant data (often terabytes in volume) from ISPs which was then transmitted in plain text format log files to Europol. Europol used these data to produce 3 378 intelligence reports and send requests on suspicious IP addresses to EU Member States as well as seven third countries with which Europol had an operational cooperation agreement.

In the UK investigators posed as members of the discussion forum and were able to identify a server which was seized, handed over to Europol for forensic examination and which revealed the personal details of all members, including date of birth, occupation and country of residence. Those Member States which had not yet transposed - Austria, Germany (which received packages of IP data related to 377 suspects), Sweden, Czech Republic and Norway, and others which lacked specific legal measures against child pornography, were unable to meet these requests because data were not available from service providers could not be or do not defined legislation or definition of written child pornography.

Of the eight EU Member States and six third countries which were able to take action, the operation identified overall 230 victims of child abuse and 670 suspects leading to 184 arrests. Two-hundred and forty of these suspects were UK residents and included police officers, teachers and youth leaders, and there have been 33 convictions. One man was sentenced in March 2010 to six years' imprisonment for sexual abuse of two minors after police discovered more than 60 000 indecent images on his computer.

Case 5 (France)

In April 2007 French Police National were charged with investigating 'MGJ-P' who had been on the run since his conviction in absentia in December 1997 when he was sentenced to 20 years' imprisonment for rape of a minor. Police took a close interest in the fugitive's family circle and in particular his mother, Mme GJ. Detailed call records for the number of Mme GJ for the previous 12 months were requested from her telephone service provider. Examination of the call records enabled the identification of a telephone number in another country ('P'). Investigations also showed that Mme GJ was sending cash through Western Union to a person who was resident in P. The interception of the telephone line of Mme GJ confirmed that she was making regular calls to her son who was living in country P. With the help of the liaison officer and local authorities in P, MGJ-P was arrested in September 2007 pending extradition to France.

Case 6 (Poland)

A major suspect in a series of incidents of sexual abuse of minors in Wrocław had managed to evade detection. After 15 months involving interviews with 40 people the police obtained the e-mail address of the offender. A list of system logs for this account was obtained that allowed to determine the IP address. Subsequently the perpetrator was identified. Police consider that without this period of retention identification would not have been possible.

Case 7 (Spain)

Spanish investigators following a report in October 2007 uncovered a string of grooming incidents between January 2007 and August 2008 in which a man pretending to be a woman or minor on various internet for a persuaded young girls to take photographs and videos of themselves of a sexual nature. He then used a software tool to send these images and videos to various email addresses using the name 'Rafael'. Traffic data were obtained from the service provider on basis of a court order in May 2008 which enabled offender to be identified, as was acknowledged explicitly by the judge in the trial in which the man was convicted of six counts of corruption of a minor.

Case 8 (Sweden)

In 2010 an eight-year-old girl was kidnapped not far from her school. She was driven away in a car and sexually assaulted before being released. At the police station the girl described the make and colour of the car, and recalled that during the assault the man had received but not answered two telephone calls. As there were too many cars fitting the description to enable accurate identification, the police requested the log of active mobile phones in the area, and identified two numbers to which there had been two unanswered calls. This led to the identification, arrest and confession of the offender who was sentenced to six-year imprisonment.

Case 9 (UK)

A 14-year old female from the Fife area was reported missing in November 2009. She had a history of self-harm and multiple suicide attempts. She had left a note for her parents in which she claimed to have been 'hearing voices'. A trace to find the live location of the victim's telephone was carried out but it had been switched off. Historical call data was examined to ascertain with whom she had been in contact prior to her going missing. The call data identified a mobile telephone whose subscription was attached to an individual unknown to the girl's parents. Checks at the registered address of the subscriber revealed that the missing girl was in the company of a 36-year-old man whom she had met in an internet chat room. The man was charged with sexual offences.

Case 10 (UK)

UK authorities received intelligence from US authorities that an individual using internet email had sent a movie file of a woman sexually abusing a four-month-old girl. The log-on IP address for this account was found to be registered to a male from Northampton. Further enquiries established that a girlfriend of the individual had three children all less than four years old. After investigation both were convicted of the serious sexual abuse of the children. The children had been found in conditions of neglect, described by an officer as filthy, unsanitary and unfit for human residence.

Case 11 (UK)

Internet data were used in an investigation into the grooming of a 13-year-old girl on an internet chat service. Examination of the victim's computer by the authorities revealed the email address of a man who had coerced the girl into sending naked photographs of herself and exposing herself during webcam chat. Police officers made enquiries about the e-mail address which revealed the IP address belonged to an address in Wales. Further investigation resulted in the man being charged preventing potentially more serious sexual offences taking place.

Buying or offering online child pornography

Case 1 (Czech Republic)

An e-mail box was suspected to be connected to child pornography and investigation (known as Operation VILMA) began through requests for access logs and e-mail addresses related to particular suspicious e-mail traffic. This revealed a network of holders and disseminators of child zoophile pornography, leading to dozens of house searches across the country and to several arrests.

Case 2 (Europol/ Spain)

Operation Atlantic was a joint investigation by the FBI and Europol over the course of a year into users of a forum for exchange and downloading of paedophile content hosted on a private peer-to-peer server. Europol distributed to France, Italy, Netherlands, Spain and UK in December 2010 information gathered by the FBI. Spanish investigators were able to resolve IP addresses which had been retained for over six months, leading to the arrest of two individuals who were subsequently also found to have sexually abused a seven-year-old. Overall, by February 2012, 37 child sex offenders had been identified with 17 arrests for child sexual molestation and production of illegal content.[28]

Case 3 (Germany)

Police in April 2010 launched an investigation into the dissemination of child pornographic images and videos. Internet research uncovered a number of temporary websites from which users could access a portal – in exchange for a payment of $200 to various Russian individuals - for purchasing child pornographic images. Investigators carried out surveillance of email accounts and stored traffic data relating to persons interested in these images over the course of a month but none of the IP addresses used to log onto these email accounts was available.

Case 4 (Luxembourg)

Police discovered a server based in Luxembourg distributing child pornography images. The server was seized for analysis. It took specialists four months to identify with certainty a total of 57890 IP addresses located in 134 different countries around the world which had been used to view or download the images. As part of the subsequent international investigation

[28] https://www.europol.europa.eu/content/press/european-police-and-fbi-dismantle-network-child-sex-offenders-1361; http://www.guardiacivil.es/en/prensa/noticias/4010.html

known as 'Operation Charly', hundreds of arrests on suspicion of child pornography offences have been reported around the EU.

Case 5 (Luxembourg)

Irish authorities obtained information from New Zealand that a child was at risk of sexual abuse by an internet user based in Ireland. Irish investigators discovered him to be exchanging child pornographic images with a user based in Luxembourg by means of instant messaging software. Two Luxembourg based IP addresses were provided to police via Europol, but the six month retention period had already lapsed and the investigation could proceed not further.

Case 6 (Poland)

In 2009, Polish authorities coordinated eight operations targeting persons distributing child pornography over the internet, using data obtained from regional police investigators, Europol and Interpol. Investigators carried out 428 searches in private houses, businesses, workplaces and internet cafes) and arrested 473 persons leading to 62 provisional sentences.

Case 7 (Spain)

Spanish police (Operation Kruna) detected a user in September 2010 distributing 65 child pornography files over a peer-to-peer network. The court order for obtaining the user and traffic data from the ISP was signed in June 2011, which enabled the location of a large volume of child pornography material.

Case 8 (Spain)

Having detected distribution of child pornography files over a peer-to-peer file sharing network to 65 users in January 2010, Spanish investigators (Operation Oslo) requested judicial authorisation to request data held by ISPs to identify the distributer. Authorisation was issued in June 2010 and led to nine arrests.

Case 9 (Spain)

Police were notified in June 2009 by Interpol of a suspected distribution of child pornography via internet servers located in Spain. In October, investigators sought judicial authorisation to access IP data, which led to the identification and arrest of three individuals.

Drugs trafficking

Case 1 (Denmark)

Police arrested a person at the Danish border for possession of 7.5 kilo of amphetamines. The person disclosed the name and telephone number of the supplier of the drugs. Traffic data, along with lawful interception of telephone calls and video surveillance led to the identification and eventual conviction of three individuals involved in an international drugs trafficking ring.

Case 2 (Denmark)

Police investigating the activities of a man suspected of organising the smuggling cocaine from Netherlands to Denmark used evidence acquired through wiretaps to seize 9 kg of cocaine and to make five arrests. Communications data connected to devices in the possession

of the individuals arrested enabled investigators to implicate the man at the centre of the smuggling activities.

Case 3 (Spain)

In 2010 Spanish police in collaboration with Paraguayan authorities carried out an investigation into an organisation dealing in the trafficking of Paraguayan women into Spain for purposes of sexual exploitation in clubs in the province of Albacete. In June 2010 Paraguayan authorities arrested two of the leaders of the organisation at the national airport. In January 2011, Spain received rogatory letters from the Paraguayan public prosecutor requesting subscriber and traffic data concerning two Spanish telephone lines between May and June 2010. The data had been retained and were exchanged in accordance with the request.

Case 4 (UK)

In 2010/ 2011 police used data from thousands of calls over the previous 12 months between more than a dozen mobile phones to dismantle a nationwide cocaine trafficking ring. Two gang members found to be in possession of 3.58 kg of cocaine (valued 165 000 EUR) were arrested and their mobile phones seized. Detectives then spent months examining communications data to identify links between the other members of the group. This resulted in conviction of six gang members who were sentenced for a total of 53 years imprisonment and the confiscation of 61 000 EUR in cash which is being used to fund police operations targeting other drug dealers.

Case 5 (UK)

Operation Frant was a detailed investigation into a number of drug dealers who were flooding London and the UK with high grade heroin from Afghanistan. The aim was to target the individuals who were masterminding this organised crime network, and as they were not 'hands on' the only possible method of detection was detailed investigation of communications data. The first part of the operation targeted the 'runners' with their consignments. In December 2007 Ghaffor Hussein was arrested in possession of a kilogramme of heroin and in January 2008 Christian Bailey was arrested in possession of 8 kilos of heroin. In April 2008 Harminder Chana and Patrick Kuster (a Dutch national) were arrested in possession of 356 kilos of heroin, having been under surveillance when the exchange took place. One of the ringleaders, Atif Khan, was also arrested later that day on the basis of telephone data and additional surveillance evidence linking him and Chana. Upon arrest all suspects' telephones were seized enabling investigators to obtain the cell site data and establish who orchestrated the deals. Mobile telephone call logs revealed that a certain telephone number had been used to call Khan's telephone 26 times, along with several texts, in a 45-minute period after Khan's arrest. This so-called 'dirty telephone' was attributed to one Abdul Rob by cell site analysis which showed two mobile phones always in the same place at the same time. The telephone evidence was crucial in the case against Rob as there was no previous surveillance evidence of association with the other members of the network. Four members of the network were convicted for conspiracy to supply heroin and sentenced for total 81.5 years imprisonment.

Case 6 (UK)

In January 2008 customs officers at Birmingham airport discovered over 16 kilos of heroine concealed with straws which had been threaded through rugs imported from Afghanistan, they

alerted the Serious Organised Crime Agency. SOCA substituted the drugs rugs with dummies, replaced the original packaging, and began a surveillance operation when the gang came to collect them. After the gang's hire car was abandoned for the second time, SOCA investigators decided to switch from traditional surveillance and to focus instead on their other main lead – a single unregistered mobile telephone number used by the gang to contact the courier company. Analysis of telephone data ultimately led to the identification of five men involved in the plot. All five gang members pleaded guilty on the strength of the telephone evidence. The four main players were sentenced at Birmingham Crown Court in June 2009 to between 10 years 8 months and 14 years 8 months and 14 years 5 months for conspiracy to import Class A drugs.

Armed robbery

Case 1 (Belgium)

In the Antwerp area at night over the Easter holidays two men broke into a second-floor apartment. The resident of the apparent was badly beaten and tied up with tape. A little while later, the same apartment block was broken into a second time, this time on the first floor. The attackers used tear gas and the resident was also tied up and blindfolded. Knowing he was an employee in the court in Antwerp in possession of keys and security code for the court registry where the evidence was stored, the attackers obtained security details. The investigation of the crime scene yielded little information on the perpetrators. The only clear DNA profiles found belonged to the victims. Authorities obtained data on mobile telephone mast traffic and compared telephone activity near the apartment building and the court, and detected two telephone numbers present at both locations communicating only with each other by text message. The numbers had been activated a week before the attacks and deactivated soon afterwards. Police established that the same communication method and activation/ deactivation activity had taken place in the same area involving a further eight Dutch mobile telephone numbers. These methods are often used to evade detection. The data were used were used to disprove the suspects' alibis, and to link the mobile phones with the suspects. The court found that the data demonstrated 'with reasonable certainty that the owners of the telephone numbers were involved' in the crime.

Case 2 (Czech Republic)

Two masked men paralysed an employee of a security firm and stole three safe boxes containing over 14 million CZK (582 000 EUR) in cash. The men used a car driven by a third individual to get away before abandoning and setting fire to the vehicle at a remote location. Czech police obtained list of active calls at the place of attack and at the place where the getaway car had been purchased. By comparing the lists some active numbers were found to be the same. This led to further investigation on other numbers that were in contact on both places with the already identified numbers. Investigators would have been severely limited in their ability to pursue the case without access to the data.

Case 3 (*Czech Republic)*

A gang robbed Raiffeisen Bank in Chomutov and during escape fired guns at the police. Czech police were able to identify the perpetrators through analysis of the telephone calls made before and after the robbery.

Case 4 (Germany)

A taxi was ordered using fixed telephone line. The taxi arrived and was hailed by a woman. The taxi then stopped, and a man jumped out of nearby bushes and pointing a gun at him demanded the taxi driver's money. Both suspects (the man and the woman) escaped with the money. The investigation has proceded no further because the telephone provider said that the traffic data had been deleted and therefore an identification of the subscriber of the calling telephone line would not be possible.

Case 5 (Netherlands)

A group of 12 individuals was suspected of involvement in several cases of armed robbery, extortion and burglary in Netherlands in 2010. Using historical traffic police detected plans by the group to raid a house in Groessen, and the four were arrested in a car while en route to the house.

Case 6 (UK)

Police investigated (Operation Backfill) a series of armed robberies where high value cars were advertised on a website for sale for 'strictly cash only'. Persons interested in buying the cars went to meet the supposed traders and were robbed at gun point. Police examined internet data and identified the laptop and premises from where the suspects had logged onto the internet when posting the advertisements, leading to a number of arrests.

Burglary, theft and organised trafficking

Case 1 (Bulgaria)

In 2012 three mobile telephone operators provided data enabling detection of leaders of an organised group dealing in illegal acquisition and sale of moveable cultural property to Germany, Austria, Spain, Switzerland, Italy and USA.

Case 2 (Czech Republic)

In 2006 there were seven incidents in the Liberec region of the Czech Republic in which three individuals would remove ATMs and take them to another location where they would remove the cash and discard the machine, causing loss and damage of 40 million CRK (1.5 million EUR). Suspecting that mobile phones were used by the gang to coordinate the robberies, police acquired data showing that in four cases the same telephone numbers were involved. Investigators were able to connect suspects to the theft overall of 24 ATMs (totalling 100 million CRK or 4 million EUR).

Case 3 (Czech Republic)

In 2008 and 2009 there were a number of robberies targeting shops in the Vsetin and Zlin regions in which goods and cash to the value of 3 000 000 CRK (120 000 EUR) were stolen. Little evidence was left at the crime scene, so police analysed data from mobile communication which revealed the presence of the same telephone number and IMEI at two of the locations, leading to several arrests.

Case 4 (Denmark)

Investigators intercepted communications using a mobile telephone which had been stolen during a burglary, leading to a police raid on an abandoned property in which a large quantity of stolen goods was discovered. Further analysis of related historical communications data pointed to four members of a family from another European country that was already under suspicion in connection with various other offences, including a homicide. The investigation led to the discovery of a container of stolen goods valued at 2 700 000 DKK (362 000 EUR), and to the extradition and charge of one of the family members.

Case 5 (Denmark)

Four masked men broke into the home of an elderly couple using threatening behaviour to steal their car and obtain the PIN numbers for their credit cards. One of the offenders was soon afterwards arrested, and communications data connected to his mobile telephone revealed those with whom he had been in contact around the time of the robbery. Location data then enabled police to place three further suspects at the scene of the crime and at the ATM machine where the stolen cards had been used.

Cases 6-8 (Germany, Hungary, Poland)

Soray P. headed a criminal group engaged in fraud by pretending to be the granddaughter of hundreds of elderly people in Germany, Austria, Italy and Poland. German police issued a European Arrest Warrant in connection with crimes involving the theft of 400 000 EUR. Polish police were able to identify and arrest in August 2011 the woman through examining data relating to various telephone numbers over the course of several months. The investigation into a similar case involving 38 incidents in the Warmińsko-Mazurskie district and the theft of 48 000 EUR between June 2009 and January 2010 led to the conviction of Adam M. In a third example, Hungarian police began an investigation into telephone fraud in which a number of elderly persons in Budapest, Tolna and other areas regions had in 2009/2010 been tricked into handing over their savings. The perpetrators were identified by telephone service provider data. German police reported a similar set of incidents which could not be investigated because of the absence of telephone data.

Case 9 (Germany)

During three months prior to a burglary, residents noted random test calls made to their landline. Immediately after the burglary was committed a court order to identify the subscriber was obtained to get hold of the subscriber. But data had not been retained by the provider and the investigation has proceeded no further.

Case 10 (Germany)

After a spate of burglaries of residential properties, investigators discovered that over two-three months irregular 'test-calls' had been made to the houses which had been subsequently broken into. Immediately after the next similar burglary, a request was made to the telephone service provider for data on the recent callers to that house, but the data were no longer available.

Case 11 (Germany)

Police investigated a series of thefts of vehicles and expensive construction machines which were dismantled and their parts sold over an internet auction site. Orders for the release of retrograde communications data regarding mobile and fixed-line phones, revealed by the police in separate cases, were issued in connection with an investigation into gang-related trade in stolen property. Historical communications data was not available. Therefore the overall structure of the gang, the individuals and their places of handover, have not been identified. It was not possible to prove the meeting points for making arrangements on the basis of the coordinates.

Case 12 (Latvia)

Latvian police were able to connect a man using an anonymous pre-paid SIM card to a spate of robberies by analysing traffic data which enabled his girlfriend to be identified. The man was convicted on 17 counts of robberies.

Case 13 (Luxembourg)

A bank employee was found to have diverted customers' funds through the use of falsified documents. The accusation was brought before the prosecutor several months after the alleged offence. The plaintiff, one of the bank's customers, cited in evidence a telephone call to the bank, in which the customer expressed a wish to transfer to another bank. Traffic data was requested and obtained two weeks before the expiry of the applicable six month data retention period. On the basis of these data the prosecutor obtained and executed a search warrant on a travel agency for the purpose of locating the suspect who was subsequently arrested. During questioning the suspect implicated two others with whom he had been in contact by telephone. It was not possible to follow up on these leads as the data was no longer available, and investigation could not proceed further.

Case 14 (Luxembourg)

Victims of what is known as 'boiler room' scam, some of them resident outside Luxembourg, were approached by telephone and encouraged to buy shares which were claimed to be rising in value. Meanwhile the criminals perpetuating the scam manipulated the stock market by buying large volumes of shares at low prices thus artificially inflating the price of the shares. Investigators were able to identify and locate the suspects through obtaining telecommunications data. For several of the victims there was a time lag before they realised that they had been defrauded and reported the crime to the police, especially for those victims outside Luxembourg. These delays and the applicable data retention limit of six months have prevented law enforcement authorities from launching an international investigation into the extent of the fraud.

Case 15 (Poland)

Authorities in Białystok investigated cases of fraudulent insurance claims for cars which had been taken abroad and then reported as stolen. Communications data confirmed that contact had been established between the owners of the cars, and the people who crossed the border with them. The prosecutor could also confirm that during the time of the alleged theft of the vehicles, the owners were not in the place that they claimed to be the scene of the crime, but elsewhere where they handed over the vehicle to their accomplices.

Case 16 (Poland)

In an investigation into the theft from the Auschwitz-Birkenau national museum in December 2009 of a part of the main gate bearing the inscription *'Arbeit Macht Frei*', police examined telephone logs from the area and identified a Swedish telephone number. Through mutual legal assistance agreement investigators obtained from Sweden data on telephone connections and subscribers, which enabled them to arrest and charge a number of suspects.

Case 17 (Spain)

Operation Olmo started in August 2009 and culminated in with the breaking up of an international criminal organisation involved in kidnappings, serious injuries, drugs trafficking, possession of illegal arms, threats, extortion, illegal detention, crimes against moral integrity, misappropriation of public office, violent robbery and intimidation, falsification of public documents, theft and break-in of vehicles, crimes against administration of justice, misappropriation of civil status, fraud and money laundering. Communications data enabled investigators to identify the time, duration and location of crimes committed leading to the trial of 34 individuals.[29]

Case 18 (Spain)

Operación Lentisco dismantled a criminal gang involved in burglaries of town halls and private properties, counterfeiting of currencies, violent robberies of industrial units and petrol stations, and extortion. Mobile telephony subscriber and traffic data were especially relevant as the gang constantly switched pre-paid cards and addresses. Twenty-two crimes were detected and 14 individuals were arrested, seven of whom were given prison sentences.[30]

Case 19 (Spain)

In 2009 a jewellers was robbed of diamonds valued at 10m EUR as result of a 'rip deal' confidence trick. It took Spanish investigators in cooperation with Interpol and police in France, Italy and Belgium six months to gather sufficient information to request court order for communications data, which eventually led to the identification and trial of seven individuals.[31]

Case 20 (Spain)

Operation Cobra dismantled an organised gang involved in burglaries disguised as police and Guardia Civil officers to gain the confidence of the victims and using balaclavas, scarves and gloves as well as signal and GPS jammers to escape detection. The leader of the group used a sawn-off shotgun in case his other intimidation methods were insufficient. Six individuals were arrested in connection with 45 incidents including one attempted homicide. Mobile telephony data were necessary to identify the culprits and their whereabouts.[32]

---

[29] http://www.policia.es/wap/prensa/20110518_1.html; http://www.policia.es/wap/prensa/20120301_1.html

[30] http://www.teleprensa.es/almeria-noticia-334247-desarticulada-una-organizacin-en-almera-especializada-en-robos-y-extorsiones-a-empresarios.html

[31] http://www.policia.es/prensa/20110629_1.html

[32] http://www.elmundo.es/elmundo/2012/02/03/andalucia/1328262438.html

Case 21 (Spain)

A series of incidents of internet fraud, falsification of credit cards and the collection, distribution and sale of stolen goods, took place in December 2007. Following a lead appearing in October 2008, police requested IP addresses which enabled the identification and location and subsequent wiretap of an ASDL, culminating in the arrest of 26 members and collaborators of a criminal gang in connection with around 500 offences.

Case 22 (Germany)

Five persons were suspected of being members of a group of smugglers. Their mobile telephone numbers could be identified but due to the absence of data retention, it was not possible to determine their location at the time of the smuggling or the identities of persons receiving calls from the suspects.

Case 23 (Sweden)

During 2003-2005 a team of at least four individuals drugged and robbed men in the nightclub district of Stockholm. They took the victims to their houses and stole everything of value and also stole money from their bank accounts. Telephone records demonstrated the suspects' presence in a number of different crime scenes throughout the period in question, and this was crucial to the prosecution of two of the perpetrators.

Case 24 (UK)

In October 2004 a large criminal network conspired to steal 229 million GBP (265 million EUR) from a bank in the City of London by transferring funds to bank accounts opened in seven different countries. Landline and mobile telephone communication data was critical to establishing those involved in this crime and understanding how it happened. The network members used landline, mobile, and kiosk phones in the UK and across multiple countries. Three defendants were extradited to the UK for trial. Billing data, call data and cell-site location data were all used as evidence in the trial which took place in March 2009. Three defendants were convicted of conspiracy to steal and two were convicted of money laundering.

Cybercrime

Case 1 (Denmark)

In March 2009 Danish police were notified by an online payment service provider that several customers' accounts had been hacked. Authorities in another state meanwhile reported that information on their credit cards had been disclosed in forums on the internet. Investigators identified three IP addresses belonging to two electronic communications service providers, which enabled the telephone service providers to identify the subscribers. This evidence led in 2009 to the conviction and sentencing to three years' imprisonment of a man for 19 separate offences, including computer fraud and attempted fraud, hacking, forgery and disclosure of stolen credit card information.

Case 2 (France)

In May 2009 a publically-funded regional body noticed a website was hosting a 'phishing' page which fraudulently redirected surfers into providing username and passwords for their

online bank accounts. A representative of the body in June 2009 reported this as an act of piracy to the French National Police. Technical queries run on a copy of the site in question revealed that the fraudulently acquired data were being sent in the form of an email to two active webmail accounts. The owners of these accounts were suspected of complicity with the pirates and a judicial warrant was issued on the webmail service. Details of access to these emails revealed a number of Moroccan IP addresses for the first account and a Paris-based company for the second. It appeared that the company was offering file-sharing services and internet anonymisation services. Interviews with the directors of the company and inspection of their equipment revealed two French IP addresses had been used to access the inbox. Investigators requested details of the user of these IP addresses from the French ISP and the response received in February 2010 identified two French nationals. Further investigation of the activities of these persons led in turn to a resident of Morocco who was profiting from the phishing page.

Case 3 (Germany)

German police received information from Luxemburg following the analysis of a seized Command and Control Server of a botnet which anonymised data and obtained the digital identities of unwitting users. 218 703 German IP addresses which had accessed this server were sent to the police to inform/warn the owners of the computers, but most of the requests for information subsequently submitted by the police authorities because the subscriber details had not been retained.

Case 4 (Poland)

In December 2009 there were a number of attempts to destroy, to damage, to remove or to hinder access to computer data being used to create a government website. The data were located on a servers administered by the Centre of the Prime Minister, the National Hydrological Services and the Geological Institute/ National Research Institute. Police arrested the perpetrator through identification of the computer's IP address.

Case 5 (Spain)

A group of hackers inadvertently installed botnet malware on around 13 million computers in various countries. This enabled between December 2009 and February 2010 the infiltration of denial-of-service actions where huge volumes of credit card data were obtained and a search engine was tricked as to the value of a web advert through the simulation of user click which in reality were automated by the botnet. Spanish police were requested by the authorities of another country to assist in the investigation, which required access to data which were up to one year old. The investigation is ongoing but at time of reporting had resulting in 10 arrests and three charges.[33]

Fraud

Case 1 (Czech Republic)

A person set up an e-shop which required advance payments but then did not deliver the goods which had been purchased. Over a short period customers were defrauded of thousands of CRK. The e-shop was operated for just a few weeks before it was shut down. The

[33] http://tecnologia.elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html

communication between the customers and perpetrator was through e-mails and electronic forms, and payments made by credit card and internet banking. Without data concerning internet access, it would not be possible to investigate this case.

Case 2 (Denmark)

In March 2009 Danish police was alerted by police in another Member State that an anonymous person had passed information on stolen credit cards in closed forums on the internet. The police launched in a background investigation of the case and identified three IP addresses that belonged to two electronic communications service providers. With a court order the North Jutland Police accessed the retained relevant IP addresses. Based on the information gathered the perpetrator was charged and sentenced to three years in prison on a total of 19 counts, including computer fraud and hacking and exchanging stolen goods.

Case 3 (Denmark)

That police were alerted by a Danish on-line payment service provider that several of their customers' accounts had been hacked and subsequently used to deposit money using stolen credit card information. The money was subsequently transferred from customers' accounts to an online poker account located outside Denmark, while a smaller portion of the proceeds were transferred to a Danish bank as winnings from online gambling. One particular IP address was used to log into all of the hacked accounts, so there was a presumption that there was one unidentified individual. It was known that this person had used various addresses in connection with registration with the online payment service provider, and the email providers were able to supply data for identifying the individual who was subsequently charged on further counts of hacking, computer fraud, forgery and the dissemination of credit card information.

Case 3 (France)

In November 2005, French National Police was charged with investigating and locating an individual, known as 'MGB', who was wanted following convictions by various courts on serious charges. The police investigations in 2006 and early 2007 centred on the family circle and close relations of MGB, and relied mainly on telephony. Interception of telephone communication did not provide any evidence of a connection between the fugitive and his family. In February 2007, the fugitive's sister, 'MB', was arrested on charges of organised fraud. The police obtained some information about the fugitive's sister, in particular her aliases and her immediate circle of friends/acquaintances. One of the aliases, 'LA', attracted the attention of the investigators. By cross-checking call records, it was shown that LA was in fact MGB. A detailed invoice for the telephone line of MGB, (registered under an assumed name) provided call data over a one year period. This enabled calls to Senegal in March 2006 to be highlighted and associated with the telephone number assigned to LA. As a result the investigation relating to the fugitive focused on calls to and from Senegal, thus enabling telephone numbers, obtained under assumed identities, to be identified as those of MGB's family. Subsequently, thanks to new judicial interceptions and the help of the in-country liaison officer in the country where he was hiding, MGB was formally identified, located, and arrested by local police in March 2007, and found to be in possession of falsified French identity documents using the alias 'LA'.

Case 4 (France)

In May 2008 police noticed an unusually large invoice caused by the diversion to premium-rate telephone lines of 10 telephone lines belonging to a ministry. These lines were being used intensively to obtain codes allowing pirates to access payable internet sites or to receive gifts. Initial investigations focused on the telephone architecture of the ministry and how it was possible to connect to it, through interviews with technicians and service providers. A large volume of information on incoming calls for these 10 lines indicated that there were 10 separate subscribers. During autumn 2008, these subscribers were identified. The details of their IP accounts were requested and obtained from the ISP in December 2008.

These data gave rise to a suspicion that two IP addresses were using a subscriber's SIP profile without his knowledge in order to connect to the ministerial private automatic branch exchange network (PABX) and to use it to call the premium rate numbers. The alleged offenders were therefore only identified in mid-December – about seven months after the discovery of the suspicious invoice.

Case 5 (Lithuania)

In 2010 a series of instances of telephone fraud were detected in Vilnius. Victims were approached by calls made from mobile telephones and were falsely informed about crimes that their relatives had allegedly committed or about disastrous events which had befallen their relatives. Victims were pressurised into surrendering money or other valuable possessions. A special police task force was set up to investigate the incidents. It took investigators several months to obtain and to analyse communications data, which enabled them to uncover a conspiracy including prisoners in Marijampole and who were involved in similar fraudulent activities in other Lithuanian towns. Eventually 18 individuals were arrested on suspicion of committing 29 counts of fraud totalling about 85 000 LTL (25 000 EUR).

Case 6 (Poland)

Polish citizens involved in the import via Germany into Poland of textiles, footwear and other goods from China and Vietnam were found to have evaded an estimated 100 million PLN (24 million EUR) per year in VAT payments. They used falsified documents and frequent switching of mobile phones and SIM cards to attempt to evade detection. Investigators' analysis of traffic data revealed connections to known members of a criminal group, and location data and IP addresses connected them to the place of delivery of the goods and computers used to send commercial documents.

DG Home

European Commission

March 2013