15.12.2009

FINNISH LAW ENFORCEMENT (NBI), TELECOMMUNICATION AUTHORITIES, DPA AND TELECOM OPERATOR ANSWERS TO THE QUESTIONNAIRE FOR THE EVALUATION OF DIRECTIVE 2006/24/EC

1 QUESTIONS TO MEMBER STATES AND BY EEA STATES

1.A Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10,

1.A.1 Law enforcement issues

1.A.1.a Total number of requests that are issued by year to obtain data retained under the DRD [Quantitative Reply]

1.A.1.b Number/Percentage of these requests that are generated by type of requesting authority: 1. police, 2. judicial, and 3. other authorities (please specify) [Quantitative Reply]

1.A.1.c What is the average age of the data that are requested? [Quantitative Reply]

National Bureau of Investigation’s (NBI) answers to questions 1.A.1.a, 1.A.1.b and 1.A.1.c.

<table>
<thead>
<tr>
<th>Historical Data requests Acquired by 2008-2009 Police</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-3months</td>
</tr>
<tr>
<td>1752</td>
</tr>
</tbody>
</table>

- 1 -
Historical Data requests Acquired by 2008-2009

Customs

<table>
<thead>
<tr>
<th>Time Range</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-3 months</td>
<td>161</td>
<td>248</td>
</tr>
<tr>
<td>3-6 months</td>
<td>216</td>
<td>265</td>
</tr>
<tr>
<td>6-9 months</td>
<td>67</td>
<td>37</td>
</tr>
<tr>
<td>9-12 months</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Over 12 months</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

Start Youngest = From the Query date how many days backwards is the first queried date
End Oldest = From the Query date how many days backwards is the last queried date
Average Query Length is a calculation between these two median days

Query time range average length by police in year 2008
Start Youngest = 77 days
End Oldest = 125 days
Average Query Length = 48 days

Query time range average length by police in year 2009
Start Youngest = 83 days
End Oldest = 110 days
Average Query Length = 27 days

Total number of requests by police since 1.1.2008 = 7050

Query time range average length by customs in year 2008
Start Youngest = 11 days
End Oldest = 131 days
Average Query Length = 120 days

Query time range average length by customs in year 2009
Start Youngest = 3 days
End Oldest = 113 days
Average Query Length = 110 days

Total number of requests by customs since 1.1.2008 = 1032

* Start Youngest = From the Query date how many days backwards is the first queried date
* End Oldest = From the Query date how many days backwards is the last queried date
* Average Query Length is a calculation between these two median days

It seems that the investigation profile differs a lot between Customs and Police. Customs are investigation more 'fresh' cases and their median for the first date is about two months fresher data than police is asking. For the Police there were in 2008 245 queries where data was requested beyond the 12 months retention time. That’s about 13.8% of the cases.

1.A.1.d Which communication channels are used to exchange information between law enforcement authorities and service providers (e-mail, fax, secure network, or other channels)? If certain channels are required to be used, please provide information about the channels to be used.

NBI: "NBI sends the requests by PGP-encrypted email or Adobe Acrobat encrypted attached email. Two largest operators deliver the content by dedicated systems. All other operators deliver by encrypted email (various methods), standard mail in certain cases (Material is included in DVD), or providing direct access to the copy of the original data."
1.A.1.e Type of crimes

1.A.1.e.1 For what types of serious crime does the national law authorise the use of retained data? Please provide a list of these crimes

NBI: "Only serious crimes defined in Coercive Measures Act Chapter 5a paragraph 3§. Main principle is: Crimes where maximum penalty is at least 4 years of imprisonment, an offence or attempt against a computer using a terminal device, pander, threatening a person to be heard by judicial authorities, menace, a drugs offence, preparation of a terrorist offence."

Ministry of Transport and Communications: “The retained data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in chapter 5 a(3)(1) of the Coercive Measures Act (450/1987). Crimes where maximum sentence is at least 4 years imprisonment or an offence directed at an automatic data processing system by using a terminal, menace, threatening a person to be heard in the administration of justice or a narcotics offence; or a punishable attempt to commit the above-mentioned offences.”

1.A.1.e.2 What is the average age of the data that has been requested for the different types of crime mentioned under I.A.1.e.1? [Quantitative Reply]

1.A.1.e.3 Does the national law allow for or prohibit acquisition of data from communications providers of data subservient of the Directive and/or related instruments for purposes other than the investigation, detection and prosecution of serious crime (e.g. copyright infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

NBI: "Can not be used to ANY other purpose. (All according to the DRD)"


However in Finland if the operator is storing the data for its own business purposes (billing, marketing, technical developing, misuse detection) it is obliged to give the data to the authority in different cases. The right of authorities to receive identification data for the purpose of preventing, uncovering or investigating crimes is laid down in the Police Act (578/2005), the Act on the Processing of Personal Data by the Border Guard (579/2005), the Customs Act (1466/1994), and the Coercive Measures Act. (343/2008) and the Act on the Protection of Privacy in Electronic Communications (516/2004).”

1.A.1.e.4 Assessment of the data to be retain
1.A.1.e.5 Does the national law transposing the Data Retention Directive or a related instrument, require the retention of other categories of data in addition to the data contained in Article 5 of the Directive? If so, please provide details about the additional data as well as the instrument in which this obligation is enshrined.

NBI: "No!"

1.A.1.e.6 Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive.

Please indicate whether the data the service providers must retain under Article 5 of the Directive are relevant and sufficient from a law enforcement perspective, and mention which data either should be removed from the list of Article 5 where redundant or be added where relevant data is not yet retained. Member States are invited to motivate their answer and provide examples of situations that demonstrate the redundancy or the law enforcement requirements.

NBI: "In Finland the original position to DRD was not to touch the existing legislation. Now even if we would have the data available in DRD database, we can not access the data which is retained, because the data is accessible only for serious crimes. The data which is described in DRD should be a minimum set which is mandatory to retain even if the operator has no use of this kind of data. The retained data is primarily for serious crimes, but the data should be allowed to be used also for investigation other crimes - simply because it exists. All data items in DRD are relevant"

1.A.1.f Details of the requests that are issued

1.A.1.f.1 The kind of information that service providers are requested to retrieve; Please provide information about the type of search parameters (information selection criteria) contained in requests for acquisition of retained data, e.g. listing of the communications made from or to a given phone number, or on certain date, or at a certain hour, or listing of all calls made from a certain location, or of all numbers used by an identified user.

NBI: "Known MSISDN \(\rightarrow\) will be searched IMEI during certain time range. Known IMEI \(\rightarrow\) will be searched MSISDN during certain time range. Known MAC-address \(\rightarrow\) user in certain very limited time range Known IP-address \(\rightarrow\) user in certain very limited time range IRI-monitoring of the MSISDN or IMEI by court order, all relevant billing data within the warrant time, which is normally for one month and it, can be extended by monthly basis IRI-monitoring of the CellID \(\rightarrow\) answer will include all active MSISDN's in certain cell location within the very limited time range (normally less than one hour)"
1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standards)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

NBI: "NBI is planning to use ETSI TS 102657 Data Retention Handover interface standard."

Ministry of Transport and Communications: “Yes.”

1.A.1.g Details of the replies to the requests mentioned under 1.A.1.g

1.A.1.h Does the national law governing the acquisition of communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as “without undue delay. If so:

NBI: "The phrase "without undue delay" is not defined any better in Finnish law. NBI is currently discussing within National working group lead by Finnish national regulator Ficora, how short these times should be. This proposal will be only recommendation and there will be no punishments of the delay. NBI's opinion is that there should be some kind of damage due the delay."

Ministry of Transport and Communications: “No.”

1.A.1.h.1 Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.

NBI: "No time frames defined. See 1.A.1.h. In recommendation there will be two types of requests: Normal and Urgent"

1.A.1.h.2 What measures do competent authorities avail of to ensure the respect of the time periods within which they request the reply to be given?

NBI: "No measures. See 1.a.1.h"

1.A.1.h.3 Where relevant, do competent authorities distinguish between time periods within which they require the disclosure of data by communication providers and the type of request or type of data they need? If so, please provide examples of such differentiation.

NBI: "No differentiation. Only difference is by which law the disclosure is requested."
1.A.1.i Reimbursement of costs

1.A.1.1 Does your country reimburse CAPEX\(^1\) and/or OPEX\(^2\) incurred by service providers? If so, please provide information about the type of costs that are reimbursed, as well as about the modalities and amount or ratio of reimbursement

NBI: "NBI will reimburse all OPEX and CAPEX."

Ministry of Transport and Communications: “Yes. The reimbursement complies with the rules that are applied in all cases when a Telco is assisting public authorities.

(1) A public authority shall implement at its own expense a system with which it may receive and handle the information. The public authority shall also be responsible for the costs of connecting the system to a communications network. (2) A telecommunications operator’s right to receive compensation from State funds applies only to the direct costs of the investment, use and maintenance of systems, equipment and software acquired to meet the needs notified by a public authority. The telecommunications operator’s right to receive compensation from State funds also covers the direct costs incurred from any measures ordered by a public authority. Decisions on the compensation for costs incurred are made by the Finnish Communications Regulatory Authority. (3) A telecommunications operator shall not use any systems, equipment or software funded by a public authority for its commercial activities.”

1.A.1.2 Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, guaranteeing a certain quality of service (request profiles, amount of requests to be handled, speed of retrieval)? If so, could you please provide information about the conditions that service providers have to meet and the link between reimbursement scheme.

NBI: "No conditions. Reimbursement scheme applies only for Telco's."

Ministry of Transport and Communications: “The implementation shall follow the principles of cost-efficiency and consider the business needs of the service operator, the technical features of the systems, and the needs of the authority paying for the costs for the retention.”

1.A.1.j Effectiveness - What is the success rate of the use of retained data

1.A.1.j.1 Did the use of retained data assist in crimes being detected and/or prosecuted within the courts that otherwise would have failed? If so, please provide examples [can entail Quantitative elements]

---

\(^1\) CAPEX or CApital EXPenditure, are expenditures creating future benefits. In concrete terms it is the cost of developing or providing non-consumable parts for the product or system, and may also include the cost of workers and facility expenses such as rent and utilities.

\(^2\) OPEX or OPerational EXPenditure are operating costs or recurring expenses which are related to the operation of a business, or to the operation of a device, component, piece of equipment or facility.
NBI: "Year 2008 there were 3405 inquiries regarding Historical data, from which 11% of the acquired information was categorised as Essential, 45% important, 26% minor relevance, and 18% no relevance at all."

1.A.1.j.2 How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment? What are the typical cost drivers? [Quantitative Reply]

NBI: "Typical maintenance costs of databases vary between 5 - 15% of the original investment. Some of the largest operators are within a yearly reimbursement scheme, from which the cost of the single question can not be calculated."

1.A.1.j.3 How can cost-effectiveness of the acquisition and use of retained data be increased? [entails Quantitative elements]

NBI: "Costs tend to lower when the acquisition scheme is highly automated. There should be more influence by LEA's, which operators are obligated to retain, especially in Finnish approach where we will reimburse CAPEX and OPEX."

1.A.2 National and transnational requests and answers

1.A.2.a Within this questionnaire, a "transnational requests" means a cross-border request for the acquisition of communications data between EU Member States and non-EU EEA States as appropriate where:

1.A.2.a.1 law enforcement authorities from other county requests you to provide data retained by service providers within your country (the "incoming requests") and

NBI: "From another country incoming requests must be granted a Finnish court order before it can be completed. Those requests are currently not calculated. No statistical information available."

1.A.2.a.2 Requests initiated by your competent authorities for data held within another country’s jurisdiction (the “outgoing requests”)

NBI: "Outgoing requests are currently not calculated. No statistical information available."

Having regard to the total number of requests mentioned under section 1.A.1a:

1.A.2.a.3 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation. [Quantitative Replies]

NBI: "No statistical information available."
1.A.2.a.4  what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]

NBI: "No statistical information available."

1.A.2.b  What is the average time to:

1.A.2.b.1 receive an answer to an outgoing request, between the moment of issuing the request and the reception of the answer (see also A.A.2.f)? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

NBI: "The time varies from 6 hours to few months if any answer is given to LEA."

1.A.2.b.2 provide an answer to an incoming request, between the moment of reception of the request and the sending of the answer? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

NBI: "Within couple day's if the information exists. There will be court decision before the request can be completed."

1.A.2.b.3 Which strategies could be deployed to reduce the time it takes to answer an incoming request?

NBI: "The time could be reduced if the court handling could be electronic warrant handling and granting."

1.A.2.c  Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?

NBI: "The investigating officer makes the decision when to make international rogatory letter inquiries"

1.A.2.d  Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.

NBI: "Yes there is one central point which has to be used. For full details, please visit the MLA Atlas of the European Judicial Network: http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx"
1.A.2.e Costs

1.A.2.e.1 If your country reimburses OPEX (see 1.A.1.k) do you reimburse national service providers in the same way for replying to transnational requests? Do you or do you plan to ask other Member States to share the costs?

NBI: "NBI will reimburse transnational requests. There are currently no plans to start billing other countries."

1.A.2.f Language

1.A.2.f.1 Does your country impose linguistic conditions to incoming requests (e.g. translation in a national or vehicular language? If so, please provide details about those conditions.

NBI: "For full details in regard to the languages accepted, please visit the List of declarations made with respect to the treaty of the European Convention on Mutual Assistance in Criminal Matters: http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=030&CM=8&DF=4/26/2006&CL=ENG&VL=1"

1.A.2.f.2 What means does your country deploy to comply with linguistic conditions imposed by other countries to outgoing requests? Do you have a central facility to provide linguistic support?

NBI: "We have translators within NBI's headoffice, who can translate all European main languages, Nordic languages and Estonian. For other languages NBI will use contract translators."

1.A.2.g Data security

Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?

NBI: "NBI has dedicated transfer lines, and PGP encryption in use. All systems must have an audit feature which collects data from the system use. All systems users have an individual userID and passwords."

1.A.3 Telecommunications authorities

1.A.3.a Allocation of tasks

1.A.3.a.1 Which national authorities are charged with tasks resulting from the Directive (for instance, as appropriate, following up with relevant service providers about applicable law, specifying content of data to be retained e.g. in CDRs, providing for certain standardisation e.g. on the basis of ETSI standards, managing reimbursement schemes, assessing the economic impact of the implementation and application of the Directive)? Which tasks are assigned to which authority?
Finnish Communications Regulatory Authority (FICORA):" - FICORA supervises the regulations concerning data retention i.e. that the operators retain the data mentioned in law and FICORA’s regulation (given by virtue of the law); - FICORA also decides the compensations to operators regarding data retention if the operator and police/NBI do not reach an understanding of the costs. - FICORA also follows standardisation activities (as does National Bureau of Investigation Finland, NBI) and these matters are dealt in FICORA’s working group where also operators are present; - Ministry of Interior (in practice NBI) has (according to the law) to discuss the implementation and application of data retention with operators in order to reach a situation where all data considered necessary by the authorities will be retained; - Data Protection Ombudsman of Finland supervises (according to the Personal Data Act) generally the legality of processing of personal data; - Ministry of transport and communications is the responsible ministry for the law concerning data retention and can give General guidance and development for the purpose of implementing the law.

Ministry of Transport and Communications: “The Ministry of the Interior is in charge of operational tasks and it is also in charge of providing the Commission on a yearly basis with statistics on using data retained. The Finnish Communications Regulatory Authority (FICORA) may issue further orders on the technical implementation of the retention obligations. General guidance and development for the purpose of implementing this Act is the responsibility of the Ministry of Transport and Communications.”

1.A.3.a.2 When did/will the respective authorities start to be operational for these tasks?

Finnish Communications Regulatory Authority (FICORA) "FICORA started certain operations already in 2005 when the directive was being drafted."

Ministry of Transport and Communications “FICORA has issued an order on the technical implementation of the retention obligations on 5th of June 2008.”

1.A.3.a.3 For each authority: Did/does the authority need to acquire additional expertise in order to perform its tasks under the Directive? Which? How was this implemented (e.g. new staff, reorganisation, special training) or how will it be implemented?

Finnish Communications Regulatory Authority (FICORA)" FICORA did not need to acquire additional expertise."

1.A.3.a.4 Does any authority collect data about the economic effects of measures required under the Directive. If the answer to this question is affirmative, please provide details about the authority as well as about the data that are collected? [May entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA):" No."
1.A.3.a.5  Does any authority mentioned under this section engage in cross-border co-operation relating to the Directive? If so, please provide details about 1. those authorities 2. the type of action or activity that these authorities undertake in this context. [may entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "FICORA has participated in couple of meetings at the Commission. FICORA is a member of ETSI and has the co-ordination role in communications sector standardization at national level. Also NBI participates in the Commission meetings and ETSI standardization activities relating to LI."

1.A.3.a.6  Do the authorities mentioned under this section gather data concerning the impact of the required measures on competition e.g. on market entry for new operators, on advantages for bigger companies? Please provide details about the kind of data that are being collected! [last par may entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "No."

1.A.3.a.7  **Centralised storage of data by Service providers**

Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. [can entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "FICORA has no detailed knowledge of possible problems."

1.B  **Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards (cfr Council Conclusions in Annex)**

1.B.1  **Law enforcement issues**

1.B.1.a  Which means (technical, operational) or measures (procedural, law-based) does your country deploy to increase the traceability of users of communication services? Please provide a description of these measures

NBI: "We can access by law all user (subscriber) information what Telco's have recorded in their own systems. It includes Payment history, Top-up information (included which bank account or credit card was used to top-up), IMEI history and forensic examination of mobile devices."

Ministry of Transport and Communications: “For example the police are allowed to receive/obtain the IMEI-codes of the mobile phones in certain situations.”

1.B.1.b  What is the scope of these means or measures in terms of contribution to increasing the traceability of users? Please provide details about the legal justification or
administrative motivation and as well as about the scope of these instruments, i.e. whether they are aiming to assist the prevention of crime, or its detection, investigation or prosecution. Which crimes are specifically addressed by the means and measures that your country deploys?

NBI: "Excluding the DR-data, all information which can help to prevent, detect, investigate or prosecute crimes can be used if the relevant laws are obeyed. DR-data is reserved only for investigating and prosecuting serious crimes - not to prevent them. That is a major flaw in DRD"

Ministry of Transport and Communications: “These measures are given when the police needs the information to carry out the prevention, detection, investigation or prosecution of the crime. “

1.B.1.c Efficiency

1.B.1.c.1 Are the measures imposed by your country efficient in terms of achieving the aim for which they have been put in place? Please provide details about results obtained as a result of the deployment of the relevant means or measures [may entail Quantitative elements].

NBI: "In Coercive Measures act chapter 5a paragraph 3§ is defined also the efficiency clause: teleaddress that is in the possession of a suspect or otherwise used by him or temporarily disconnect such teleaddress, if it could be assumed that information obtained by identifying the call-associated data … are highly significant to the investigation of the offence."

1.B.1.c.2 Did your country assess the effectiveness of the measures? If so, please provide details of this assessment.

NBI: "Yes, annual report is given to Parliamentary Ombudsman and the Finnish Parliament"

1.B.1.c.3 What is the added efficiency of the measures deployed by your Member State in terms of improvement of your capabilities to detect, investigate or prosecute of terrorism and other serious forms of crime that go beyond the results obtained with the data obtained under Article 5(1)(e)(2) of the Directive and in particular its paragraph (vi)? [can entail Quantitative elements]

NBI: "By forcing Telco's to retain all the data which is described in DRD even if they don't have any own use for it. Data to be retained is for LEA's only. The retained data should be available for all LEA purposes including prevention and detection of crimes. The basis for the retention is that the data is available for serious crimes, but it should be available to all other crimes also. The limitation of use should not be obeyed if other national requirements to access data are fulfilled"

1.B.1.c.4 What are the costs or these measures for the private sector? [can entail Quantitative elements]
1.B.1.d  Should measures be taken at European level to increase the traceability of users of communication devices? If so, which measures should be taken, at European level? How would these measures improve the efficiency of the means and measures that you deploy at national level?

NBI: "Not necessarily"

Ministry of Transport and Communications: “None.”

1.B.1.e  Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them in attributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?

NBI: "Police academy of Finland arranges several training courses of the investigation of Call associated data handling and analyses."

1.B.2  Telecommunications authorities

1.B.2.a  Which impacts on the market do the means or measures mentioned in section 1.B.1 have?

Finnish Communications Regulatory Authority (FICORA):" FICORA has no knowledge of possible impacts."

Ministry of Transport and Communications: “It should not have any.”

1.B.2.b  Does the authority mentioned in 1.A.3.a. & monitor and enforce national measures on providers or other stakeholders?

Finnish Communications Regulatory Authority (FICORA): "FICORA supervises that the operators comply with the regulations in the Communications Market Act. In the section 95 of the act it is stated that:

"A telecommunications operator shall equip its communications network and communications service with technical instruments and features that allow the interception of electronic communications and telecommunications monitoring as referred to in the Coercive Criminal Investigation Means Act (450/1987), the Police Act (493/1995), and the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union."
1.B.2.b.1 **Did the authority mentioned in the previous question investigate any cases of non-compliance with national means or measures? Please provide details, if relevant.**

Finnish Communications Regulatory Authority (FICORA) answers to questions 1.B.2.b.1 and 1.B.2.b.2

1.B.2.b.1. Finnish Communications Regulatory Authority (FICORA): "No."

1.B.2.b.2. Finnish Communications Regulatory Authority (FICORA): "In Finland the prepaid users are not obliged to register themselves."

2 **QUESTIONS TO THE EUROPEAN PARLIAMENT AND CIVIL SOCIETY**

2.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10

2.A.1 Which has been the effect on civil liberties of the use of data retained under the Directive?

2.A.2 Which additional measures (administrative, technical, legal, or other) would be appropriate of offset the negative impact(s)?

2.A.3 Which ones of the measures mentioned under 2.A.2 should be addressed at the level of the European Union?

2.A.4 Should the balance between enhancing security by means of retaining communication data and protecting civil liberties been stricken in a different manner. If so, please provide details how to ensure a better balance as well as the motivation underlying the policy choice. [can entail Quantitative elements]

2.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure the traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards.

2.B.1 Which has been the effect on civil liberties of measures taken at national level to increase the traceability of users?

2.B.2 Which additional measures (administrative, technical, legal, or other) should be taken of offset the negative impacts?

2.B.3 Which ones of these measures should be addressed at the level of the European Union?
3 **QUESTIONS TO NATIONAL DATA PROTECTION AUTHORITIES AND THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)**

3.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10

Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

Finnish DPA (Data Protection Ombudsman): “DR-directive has been implemented in Finland with amendments to The Act on the Protection of Privacy in Electronic Communication (14 a -14 c §) which is "lex specialist" as regards the Personal Data Act (based on directive 95/46/EC). In that Act of Electronic Communication there is no task nor competence granted to the national DPA and that why major supervisory authority is FICORA on the issues.

However there might be issues relating to Data Protection which is not covered by the Act of Electronic Communication and we should apply general Personal Data Act. For the time being these possible issues has not been clarified for us.

The major impact of Finnish DPA on these issues might therefore be in those cases where criminal investigation has been started on misuse of traffic data stored on the grounds of DR-directive.

According to penal code chapter 38 paragraph 10 prosecutor and court have to ask DPAs statement on possible violation of Data Protection Rules in general. At the moment we have not made any statement related to these issues.

Finally there is Parliamentary Ombudsman in Finland who has special competence concerning supervision of the use of coercive means related to telecommunication.”

3.A.1 Do authorities have investigative powers *vis-à-vis* providers and have there been any cases of complaints etc that have led to supervisory or investigative activities?

Finnish Communications Regulatory Authority (FICORA): "FICORA supervises the regulations concerning data retention i.e. that the operators retain the data mentioned in law and FICORAs regulation (given by virtue of the law). According to the law FICORA is entitled to gain information from the operators and if the operator has not conformed to the law FICORA may order the operator to rectify the error or omission.

FICORA has had one complaint from a citizen concerning a situation where the operator had not retained the data of a user of a dynamic IP-address.”

3.A.2 Do authorities have investigative powers *vis-à-vis* public authorities and have there been any cases of complaints etc that have led to supervisory or investigative activities?
Finnish Communications Regulatory Authority (FICORA): "FICORA has no investigative powers on public authorities concerning the laws implementing the directives in question."

3.A.3 Do authorities have the power to audit the compliance of providers and have there been any audits? If so, please provide details about such audits. [can entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "According to the section 124 of the Communications Market Act FICORA has the right to perform a technical inspection of a telecommunications operator in order to supervise compliance with the obligations imposed by the Communications Market Act. The detailed data retention or data protection regulations are not in the fore mentioned act but there is a general data protection and data security obligation also in the Communications Market Act.

FICORA has not done any audits especially concerning data retention regulations."

3.A.4 Which problems have supervisory authorities observed with the practical implementation of the Directive? (legal, practical, other; please provide details) [can entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "FICORA has identified both legal challenges and practical challenges. The practical challenges result from both legal challenges and lack of resources both at the operators and NBIs side.

Law came into force too late (1st of July, 2008) and resulting from the last minute changes made in parliament, the data retained according to data retention sections of the law can only be used in investigating serious crimes. So the data retention data can not be used in all crime investigation nor by operators themselves. This leads to many practical questions/challenges, which still remain unanswered. The problems mainly relate to internet data, because operators store data from call services all ready before data retention."

3.A.5 Do authorities have experience with the supervision of data that service providers have stored centrally, i.e. either within their jurisdiction or beyond? If so, please provide details about the challenges met in that context, also with regard to data stored outside of the EU/EEA. Please specify in particular the data protection issues that have been addressed that that context and the approach that has been followed to settle the contentious issues. [can entail Quantitative elements]

Finnish Communications Regulatory Authority (FICORA): "The central storage system is not in use in Finland at the moment."

3.A.6 Please provide details about case law (jurisprudence), if any, with regard to the implementation or use of the Data Retention Directive or concerning the use of retained data?
Finnish Communications Regulatory Authority (FICORA): "FICORA has had one complaint from a citizen concerning a situation where the operator had not retained the data of a user of a dynamic IP-address."

3.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards.

Finnish Communications Regulatory Authority (FICORA): "In Finland the prepaid users are not obliged to register themselves."

3.B.1 Please provide details of the observations made by the data protection authorities with regard to practical needs and privacy issues concerning the traceability of users, in particular of mobile pre-paid SIM cards. In case any procedure has been brought against the such means or measures deployed in your country, please provide details about this procedure. [can entail Quantitative elements]

4 QUESTIONS TO THE PRIVATE SECTOR (ISPS, TELECOM OPERATORS, NETWORK AND CABLE OPERATORS)

4.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10.

For all questions in this section, please differentiate by type of service if applicable

4.A.1 Does the implementation of the Directive require that operators retain data for a longer period than allowed for business purposes under Directive 2002/58/EC?

TeliaSonera Finland:” Yes, Mobile data 7 months extra and IP data 9 months extra compared to business requirements”

4.A.2 Do national authorities oblige all operators, e.g. regardless of size, customer type and number, type of service? If differentiation is applied, please describe the criteria.

TeliaSonera Finland:” Mostly yes… but detailed specifications for retaining data are still open”

4.A.3 Since when are data retention obligations in force in practice?

TeliaSonera Finland:” The specifications for DR implementation in TeliaSonera Finland are almost ready and negotiating with authorities are in progress. The implementation phase will be during 2010”
4.A.4 Did/Will operators have to invest in infrastructure in order to fulfil their obligations on?

4.A.4.a Retaining the data for the period required by national law,

TeliaSonera Finland:” The cost estimate for implementing requirements for mobile data (including call attempts) is approximately 500 000 €. The cost estimate for implementing IP requirements for IP data is not clear yet, but will probably be between 100 000 € and 300 000 €”

4.A.4.b Ensuring the security requirements imposed by the Directive,

TeliaSonera Finland:” No extra costs”

4.A.4.c Responding to requests without undue delay, as defined by national law,

TeliaSonera Finland:” There are some cost effects but those are difficult to separate from total costs”

4.A.4.d Ensuring that data are only retained for the purposes defined in the Directive and separated from data used for business operations, if necessary.

TeliaSonera Finland:” There are some cost effects but those are difficult to separate from total costs

4.A.5 Did/Will operators have to implement specific organisational measures and procedures in order to comply with their obligations (see previous question)?

TeliaSonera Finland:” There are no significant effects on organisation or processes”

4.A.6 Is it possible to quantify financial impacts of the necessary measures? If so, please provide the relevant information to assess this impact.

TeliaSonera Finland:” If this refers to the previous question, then no?”

4.A.7 Does the reimbursement by national authorities, if any, cover the expenditure necessary for compliance with the Directive?

TeliaSonera Finland:” Yes… ALL”

4.A.8 Does necessary legislation and practice provide legal certainty to providers with respect to their obligations concerning the protection of data of their subscribers and users?

TeliaSonera Finland:” Yes”
4.A.9 Have providers received direct requests from authorities in another Member State than that of their establishment? Were their any problems with these requests?

TeliaSonera Finland:” No, all requests from authorities in another Member State comes via our national authorities”

4.A.10 Please provide information, differentiated by type of operator etc concerning the elements of section 1.A.1 of this questionnaire.

TeliaSonera Finland:” There hasn’t been any DR related request yet because the implementation of DR requirements hasn’t been done yet”

4.A.11 Which economic effect do providers observe

4.A.11.a On competition,

TeliaSonera Finland:” No effects because of full cost compensation of Finnish authorities”

4.A.11.b Investment in new infrastructures and services,

TeliaSonera Finland:” No effects because of full cost compensation of Finnish authorities”

4.A.11.c Retail tariffs? Please provide quantitative information, and where such is not possible, qualitative indicators to allow assessment of the economic effect.

TeliaSonera Finland:” No effects because of full cost compensation of Finnish authorities”

4.A.12 Centralised storage of retained data

4.A.12.a Do operators store data at a centralised level outside of the country where the data are generated? If so please provide details about the centralised storage

TeliaSonera Finland:” No”

4.A.12.b Does operators transfer retained data that are stored at centralised level to other countries that are bound by the Data Retention Directive or to third countries?

TeliaSonera Finland:” No”

4.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards
4.B.1 In how many cases have providers been requested to identify users of pre-paid SIM cards? Which types of requests (find name based on number, or number based on name etc)?

TeliaSonera Finland:” The requests of prepaid user information is asked quite often by authorities but only in very few cases we have that information stored because Prepaid users are not obligated to give any user information to operators”

4.B.2 Which means do providers have to identify users of prepaid SIM cards?

4.B.3 How effective are these methods, i.e. in which percentage of cases could the user not be identified?

4.B.4 Please compare to the same questions for contractual (post-paid) customers.
Annex

Council Conclusions on combating the criminal misuse and anonymous use of electronic communications

2908th JUSTICE and HOME AFFAIRS Council meeting Brussels, 27-28 November 2008

The Council adopted the following conclusions:

"THE COUNCIL OF THE EUROPEAN UNION,

RECALLING the importance it attaches to the development in the territory of the European Union of electronic communications and of roaming, which are corollaries of the principle of the free movement of persons and of the establishment of a real "People's Europe";

WELCOMING the efforts of the European Commission, the Member States, national regulators and providers of electronic communications to improve communications between users, in particular through roaming agreements;


RECALLING that the free movement of persons and the development of electronic communications must go hand in hand with the establishment of an area of freedom, security and justice, one of the substantive objectives of the European Union;


EMPHASISING the importance of the rules contained in the abovementioned instruments for both the protection of data derived from electronic communications and the conservation of such data for the purposes of criminal investigations;

DRAWING ATTENTION to the fact that organised criminal groups take advantage of the implementation of the principle of free movement of persons and the development of electronic (and especially mobile) communications to conduct their criminal activities in the territory of the Union;
NOTING that the impossibility, for the competent authorities, of identifying users of mobile telephones working with prepaid SIM cards can allow perpetrators of criminal offences to communicate with co-perpetrators or accomplices with complete impunity;

NOTING also that cross-border crime can be facilitated by the fact that, in roaming, the identity of the subscriber of the telephone line, registered with the home operator, is unknown to the host country operator registered in the destination country, whether that line operates on the basis of a subscription or a prepaid SIM card;

CONSIDERING the advantage there would be in being able to know the identity of the purchaser of a prepaid SIM card, in order to trace the user of a terminal;

EMPHASISING furthermore that mobile telephony is the medium of numerous criminal offences against mobile phone operators such as fraudulent reloading of prepaid phone cards and VAT fraud;

INSISTING that the development and intensification of police and judicial cooperation in criminal matters in European Union territory must be accompanied by improvements in the partnership between the public and the private sectors;

BEARING IN MIND its conclusions of 8 May 2003, in which it considered that the tracing of the use of prepaid mobile telephone cards could improve criminal investigations and particularly those relating to serious criminal offences,

CONCLUDES THAT IT IS NECESSARY TO COMBAT THE CRIMINAL MISUSE AND ANONYMOUS USE OF ELECTRONIC COMMUNICATIONS, AND TO THAT END:

RECALLS the importance of making the best possible use of the potential offered by the abovementioned European instruments;

INVITES Member States to supply, at the request of the Commission, all relevant information on legislative and non-legislative measures or technical solutions implemented to identify users of communications media, and their degree of operational effectiveness;

INVITES the Commission, in the context of the report referred to in Article 14 of the abovementioned Directive 2006/24/EC, and by 15 September 2010, to inform it of the legislative and non-legislative measures or technical solutions notified by the Member States and, on that basis, to propose non-legislative and technical solutions to help the services and authorities responsible for compliance with the law to better identify users of electronic communications services such as users of mobile phone lines opened with prepaid SIM cards and, if after evaluation it is apparent that these measures are unsuccessful in effectively ensuring traceability, to propose legislative measures;

SUGGESTS that these proposals also address the question of the reasonable retention period for information necessary to identify the phone user, given the time required for criminal investigations and in particular for those relating to serious forms of crime;
STRESSES that these proposals must take account of the objective of keeping the processing of personal data to a minimum and of using anonymous or pseudonymous data where possible, pursuant to the abovementioned Directive 2006/24/EC;

STATES that it is important that these proposals take account of their cost in relation to their anticipated benefit, and of a fair balance between the needs of the authorities and services responsible for criminal investigations and the economic development of operators and distributors bearing in mind the constraints which already weigh on them;

HOPES, finally, that the Commission proposals will, if appropriate, address any other difficulty encountered by Member States or their competent authorities in the framework of criminal investigations relating, in particular, to serious forms of crime, as regards the traceability of electronic communications, whether mobile or not – for example, difficulties relating to instant messaging used from a portable computer."