Statement

Submitted by Swedish Security Service experts in the data retention inquiry, Senior Policy Advisor Kurt Alavaara and Chief Legal Advisor Per Lagerud

General comments about the proposals

Introduction

The ability to combat crime is hugely dependent on the obligation to retain all data encompassed by the Electronic Communications Ordinance. The proposal submitted by the inquiry chair would substantially decrease the obligation to retain data, and therefore significantly reduce the possibilities of preventing, detecting, investigating and prosecuting crime. The consequences of this could be very serious in many cases. We are hereby submitting our opinion in the drafting phase of this legislation in order to explain the effects of a decreased obligation to retain data, and to emphasize how important it is for Sweden to strive for a data retention requirement within the EU that meets national needs for effective and lawful methods to combat crime.

The purpose of the data retention obligation

Serious crime causes great damage to individuals and to society as a whole. The possibility of preventing crimes in their planning stages and of investigating and prosecuting crimes once they are committed is of tremendous value. It is therefore important that the best tools possible are available to investigate and prosecute crime, for the sake of society

as a whole, its citizens in general and for the victims of crime in particular.

Allowing law enforcement agencies and security services access to communications and location data is essential to effectively combating serious crime and crime that poses a potential threat to national security. The inquiry chair states that without access to adequate investigative tools in the electronic communications environment, law enforcement agencies and security services would not be able to investigate and prosecute certain cases of serious crime, meaning that the victims of these crimes would be left unprotected by the criminal justice system. Certain crimes would thereby essentially be exempt from punishment and many plaintiffs would not be able to obtain redress. The inquiry chair also states that the nation is obligated to protect the privacy of its citizens and to protect them from intrusions of this privacy by other individuals. Should such intrusions occur, the state is obligated to ensure that these crimes are investigated. According to the inquiry chair, not allowing law enforcement agencies and security services the possibility to effectively carry out criminal investigations in an electronic/digital context would be inconsistent with Sweden's international commitments.

Communications data and location data have become an increasingly important tool in combating crime. Nowadays, when most criminal activity leaves some sort of digital trace, such information has become essential, both for intelligence-gathering efforts and in criminal investigations, and is used in nearly every investigation of serious crime. Furthermore, such information is often the first and only key to moving the investigation forward. Without that key, the door to investigative success will in many cases remain closed.

Legislative provisions contained in e.g. the Code of Judicial Procedure concerning access to communications data and location data are designed to allow law enforcement agencies and security services access to information for the purposes of determining:

– *who* has communicated with whom (i.e. the source and destination of a communication). This can be determined from data regarding phone numbers and IP addresses (telephony), email addresses, IP addresses, SMS numbers and MMS numbers (messaging), and IP addresses (internet access).

– *when* the communication took place. This can be determined from data regarding dates, traceable starting and ending times (telephony and messaging), and logon and logoff times (internet access).

– *where* the communication took place. This can be determined from location data (telephony, messaging [indirectly through IP addresses], internet access and internet capacity).
– *how* the communication took place, e.g. whether fixed telephony (including fixed IP telephony), mobile telephony (including mobile IP telephony), text messaging, MMS, email, or a call redirection function has been used.

The obligation to retain data was introduced in order to assure that such information would be accessible through lawful intrusive measures for the purpose of combating crime. This assurance would not be possible with a decreased obligation to retain data, which would mean that law enforcement agencies and security services, in their efforts to combat serious crime, would have to leave it up to chance that operators have stored such data, e.g. for billing purposes. This would have serious consequences in many cases, especially in view of the fact that even under the current data retention obligation only a minimum of strictly necessary information may be retained.

It is not necessary to restrict the obligation to retain data

The judgment by the European Court of Justice (CJEU) was based on the premise that Swedish legislation "...provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication..." (Item 97). That description is incorrect. As the inquiry chair states, the CJEU interpretation could be due to the wording of the questions (Item 51) it received from the Administrative Court of Appeal of Stockholm, Sweden, and it is therefore necessary, as the inquiry chair states, to interpret the CJEU conclusions in light of how the questions posed by the Administrative Court of Appeal were phrased.

Many of the communication methods currently being used by "modern man" and much of the communications and location data that the operators handle are not subject to the data retention obligation. This obligation does not, for example, apply to the following:

– online surfing (visiting websites),
– communication between two IP addresses when this is not telephony (e.g. calls via Skype or Viber),
– internet-based email, such as Hotmail or Gmail,
– FTP (client-server file transfers),

– chats (messaging services),
– iMessage (messaging service),
– social media services (such as Facebook, Twitter, Viber, WhatsApp, etc.), and
– community information services (such as eBay, etc.).

Nor does the data retention obligation apply to the following:

– positions when messages were sent and received,
– positions during mobile phone calls,
– positions for fixed telephony,
– equipment identities used to send and receive messages,
– equipment identities used for fixed telephony,
– subscriber identities used to send and receive messages,
– subscriber identities used to access the internet,
– information about calls not made with regular phone numbers (including the caller's and recipient's number, time and position),
– information on the port and the local IP address (i.e. the address between the subscriber and the internet service provider) for internet access, messaging and IP telephony,
– information about calls that cannot be connected because of technical problems, etc. (including the caller's and recipient's number, time, equipment and position), and
– pure location data (positions not associated with communication or internet access).

It is therefore quite apparent that the current obligation to retain data, even when it was first imposed, was restricted to a minimal list of what must be retained in order to fulfil the most rudimentary requirements of what is needed for investigations of serious crime. Also, due to advances in technology, the relative size of this minimal list keeps decreasing in relation to the amount of communications and location data that operators must handle and the number of available methods of communication. Therefore, in our view, retaining data is already the exception rather than the rule.

It is clear to us that the CJEU judgment is based on mistaken premises about how the provisions are used vis-à-vis the current technological situation and the rapid advances in this area. The obligation to retain data does not by any means apply to all information and all means of communication. Therefore, although we understand the reasoning behind the inquiry chair's interpretation of the decision, we believe that there is scope for keeping the current data retention obligation.

Restricting the data retention obligation could have very serious consequences

Following the CJEU judgment, operators have largely stopped retaining communications and location data for the purposes of combating crime. Instead, they follow the stipulation in the Electronic Communications Act that data must immediately be removed when it is no longer necessary in the operator's business operations.

Having access to all the information encompassed by the data retention obligation is vital to the maintenance of Sweden's ability to counter serious crime and protect national security interests. Such access fulfils the rudimentary requirements of what is needed in this context. The implications of further restrictions on this access would in many cases be very serious.

The negative effect that further restrictions would have is not limited to the ability of Sweden alone to combat crime. Serious crime often occurs across borders, meaning that international crime-fighting efforts would also be affected. Perpetrators sometimes travel between countries or have contacts with or are directed by individuals in other countries. The international cooperative efforts to combat crime are very extensive and would be very negatively affected if it were no longer possible to find Swedish links in cross-border serious crime or to help foreign authorities when they submit a request to Sweden for mutual legal assistance.

One of the reasons that communications and location data is of such great importance in investigations of serious crime is the uniqueness of this information – it cannot be obtained by other methods. Law enforcement agencies and security services have no other working methods that would compensate for this lack of information.

While information regarding location could in some cases be obtained via physical surveillance instead of via location data from an operator, this method is very limited and resource extensive and can hardly be considered an alternative to the information operators are able to provide, but rather sometimes as a complement. The inquiry chair also stated the obvious in that it is not possible to replace the collection of historical communications and location data with physical surveillance in real time.

It is also sometimes stated that forensic examinations of phones and computers is another method for law enforcement agencies to obtain information. This is only partly true. Firstly, seizure of property is an intrusive measure that may only be used during criminal investigations in Sweden and not to collect intelligence. Secondly, there is no

guarantee that phones or computers associated with criminal activities will be found and seized during such a search. Third, the seizure is not kept secret from the owner of the item/s. Fourth, information obtained from communications and location data often provides the legal and practical basis for carrying out successful searches, seizures and other measures in the first place. Fifth, information retrieved from the phone or computer is sometimes not completely identical to that received from operators. Sixth, a phone or a computer could be encrypted, making the information it contains inaccessible.

The chain of information must remain intact

The provision of electronic communication services is different from the past when there was only one operator on the market: the telephone services supplier Televerket [former public agency that used to have a monopoly over the provision of telecommunications services]. Currently, each communication can occur via many different operators. For example, a person could have three different subscriptions with three different operators, one each for fibre broadband, internet access and IP telephony, with each operator handling only the data concerning their own part in the communication chain. In order to piece together this communication chain, law enforcement agencies and security services must be allowed access to information from each successive operator in this chain. The information from each operator can thus be regarded as the links that law enforcement agencies and security services need in order to carry out their work successfully. If the retention obligation for a certain type of data were to be removed, it would be impossible to discover the connection between the operators. This was also mentioned by operator representatives, in the inquiry concerning communications data, as a precondition for being able to trace the parties of a communication (SOU 2007:76). The existing minimal list is also based on being able to follow communication chain.

As an example of this, the inquiry chair's proposal means that IP addresses used for internet access will be stored but that IP addresses used for telephony and messaging will not be stored. Therefore, if law enforcement agencies and security services have access to an IP address that is used by a certain person for internet access, it would be virtually impossible to link this address to the telephony and messaging services supplied by another operator. This means that it would not be possible to find out who the person communicated with or when, where and how this communication took place. It is often possible to establish the chain

of communication thanks to the logical content of the minimal list. Links would be missing in this chain if the obligation to retain certain types of data were removed. This could have more wide-reaching negative effects on combating crime than might initially be expected. It is therefore important to carefully consider the negative consequences a removal of the obligation to retain certain types of data might have.

Other comments on some of the proposals

As the inquiry chair mentions concerning the question of targeted retention, it is very difficult to know in advance when, where and by whom serious crime will be committed. Advance targeting of data retention to certain times, areas or individuals is not usually a useful method. We agree with the inquiry chair that, in a comparative sense, having the possibility of targeting data retention would not be very useful. We also agree that targeted data retention would entail considerable intrusion on the privacy of the affected individuals and that secrecy concerns would principally bar the implementation of this measure. The reason for the latter is that both private individuals and government agencies' activities would probably be negatively impacted if the information had to be submitted to all of the approximately 600 operators in Sweden and their employees. Targeted retention, as set out by the CJEU, would therefore place obvious restrictions on crime-fighting efforts. We also agree with the inquiry chair's interpretation of CJEU opinion 1/15 of 26 July 2017 concerning the possibility of systematic retention of Passenger Name Record (PNR) data.

In addition, we agree with the inquiry chair's assessment that the CJEU judgment does not concern subscription data but only communications and location data. When it comes to changes in the decision-making process in matters concerning the use of lawful interception for intelligence purposes, we agree that such decisions should be made by a prosecutor. We also welcome the suggestion that law enforcement agencies' and security services' access to this data continue to apply to data that the operators retain for their own purposes and that data may not be retained outside Sweden.

We also have a positive view of the inquiry chair's proposal that the operators' own choice of technical solutions, i.e. using Network Access Translation (NAT), should no longer impede identifying which IP address a user has been assigned. The Swedish Security Service knows of cases where injured parties could not be identified because it has not

been possible to link their IP addresses to an identifiable individual. We consider this very unfortunate.

It is imperative that provisions concerning the obligation to retain data come into force as soon as possible: at the latest on 1 July 2018.

Further information on the impact on the Swedish Security Service

The Swedish Security Service works to counter highly capable actors

In the report, the inquiry chair mentions that the obligation to retain data is already so limited that individuals with a high level of security awareness are able to communicate without leaving any digital traces of the kind that are encompassed by this obligation, and therefore the limitations proposed by the inquiry chair will not have any effect on the possibility of investigating crimes involving such individuals.

A very large portion of the criminal investigations and the intelligence investigations carried out by the Swedish Security Service feature highly capable actors who are trained and driven by foreign powers or large (e.g. terrorist) organisations. In many cases, these actors have been specially trained to conceal any digital traces they may leave behind. The Swedish Security Service's work in such cases is based on finding and analysing the communication patterns these actors use, as well as irregularities and mistakes in these patterns, and determining what conclusions can be drawn from this information. These patterns, irregularities and mistakes are often detected and can prove to be decisive to the Security Service's subsequent course of action. This is key to efforts to counter actors who are trained and aware that their criminal activities are being monitored. The negative impact on these efforts would be great if the possibility of accessing communications and location data were to be reduced. The conclusion of the inquiry chair is therefore incorrect. In summary, limiting access to communications and location data in the Swedish Security Service's work against highly capable, systematic, resourceful and persistent actors could have very serious consequences on the national security of Sweden.

The information is essential, also in intelligence activities

Criminal investigations are retrospective: law enforcement agencies and security services attempt to clarify what happened at a certain time. Intelligence activities are mainly prospective: law enforcement agencies and security services assess what might happen in the future with a view to preventing and averting crime and to detecting previously unknown crime.

As opposed to the Swedish Police, the Swedish Security Service seldom receives reports from the public on crimes that have already been committed. Instead, the Service is responsible for carrying out intelligence work in order to 1) discover individuals and groups of interest as well as phenomena, incidents and moduses that already constitute or may evolve into criminal activities with a possible impact on national security, and 2) assess incoming tips and information on threats. For this reason, the Swedish Security Service's counter-intelligence and counter-terrorism efforts are highly concentrated on intelligence work. In this work, information is gathered and/or received from many different sources. The information is then processed and analysed and an assessment is made of what has emerged. When it is deemed necessary, the conclusions are communicated outside the Service, mainly to Swedish or foreign government agencies. The purpose of this work is to prevent and avert crime or at least detect inchoate crimes. The ultimate goal is to assess how imminent any threats are and to confirm or dismiss suspected threats. This assessment is often time critical.

To illustrate this intelligence flow, where communications and location data are essential to analysis and assessment, we have chosen to include some real life examples of information that the Security Service quite often receives from members of the public as well as from Swedish and foreign government agencies. In several cases, there is information on a named individual and a specific location. In the examples below, this classified information has been excluded.

– NN was present when a person was asked to carry out an attack against [a certain place in Sweden]

– NN has been assigned with making a bomb and detonating it at [a certain building in Sweden]

– NN has provided information to ISIS attack planners

– NN is planning to carry out an attack at an unknown place in Sweden and has access to weapons

– NN sympathises with ISIS and is trying to obtain submachine guns

– NN has fought for ISIS and is building up a network in order to plan an attack in Sweden
– NN wants to get a bomb and kill people in Sweden
– NN is going to plant a bomb in [a Swedish town]
– NN is going to avenge [certain individuals] at [a certain place in Sweden]
– NN wants to use hand grenades against [certain individuals]
– NN is a member of ISIS, is behind a number of attacks and is in hiding in Sweden
– NN comes from [a certain country] and is ready to "work" in Sweden
– NN has been assigned by ISIS to carry out an attack in Sweden
– NN wants to plant bombs [at certain places in Sweden] and get rid of [certain people]

Gathering information on individuals' contacts and patterns of movement – which makes it possible to link actors, places and times – is central to intelligence work. Communications and location data are a very important and often essential part of this work. As the Swedish Security Service has already mentioned, this data is invaluable in its work (SOU 2015:31, p. 87). The government has also stated that the Swedish Security Service obviously requires this data in order to carry out its counter-intelligence and counter-terrorism work (government bill 2016/17:186, p. 9). Analysis results can be used as a basis for strategic decisions and deployment of operational measures by the Swedish Security Service or others in order to reduce confirmed threats, prosecute crimes, etc. No longer receiving communications and location data would significantly reduce the Service's ability to e.g. assess the attack threats implied in the examples above and in the worst case this would result in terrorist crime that could have been prevented.

In view of this, it is of great importance that discussions concerning the scope of the data retention obligation are equally focused on intelligence activities (which are meant to avert crime and prevent it from being committed in the first place) as on investigative activities. This is especially relevant considering that the inquiry chair states that the negative impact a reduced scope would have on intelligence activities would not by any means be possible to compensate for by using other measures. The inquiry chair is also of the opinion that the effect of a reduced scope would be greater on intelligence activities than on investigative activities. In the view of the Swedish Security Service, these conclusions are valid.

The obligation to retain data, and access to all the information this encompasses, is strictly necessary

In spite of the fact that for the purposes of this inquiry the Swedish Security Service has ranked the importance of the communications and location data, giving certain types of data a higher ranking than others, it must be emphasised that the obligation to retain data, with all the information included in this obligation, is strictly necessary to the work of the Security Service, not only for intelligence activities but also for counter-intelligence and counter-terrorism investigations (including counter-subversion).

Although it might be obvious, it is important to state here in order to avoid any misunderstanding that all types of data are not strictly necessary at the same time in every investigation. Even if the need for this data varies from case to case depending on e.g. the type of crime in question and who is implicated in this crime, the obligation to retain data and all the information included in this obligation, is vital for the Security Service's work in combating the type of crime that poses a threat to national security.

As already mentioned, following the CJEU judgment, operators have essentially stopped retaining communications and location data for the purposes of combating crime. Instead, this data is erased when it is no longer required in the operators' business activities. This has seriously hampered the Security Service's efforts to protect the security of Sweden. It has become more difficult to combat unlawful activities carried out by foreign powers against Sweden. In addition, it has not been possible for Sweden to maintain its ability to detect terrorist networks and prevent terrorist attacks.

National security

The Swedish Security Service is tasked with handling crimes related to the national security of Sweden. In the government directive to the inquiry chair (Directive 2017:16), it is stated that the effect the judgement would have on activities that lie within the remit of the Swedish Security Service is an issue to be given particular consideration. As the inquiry chair states, the CJEU judgment allows for somewhat more permissive regulations as far as national security is concerned.

The terrorist threat to Europe has escalated since the CJEU judgment was issued; a terrorist attack was carried out in Sweden in April 2017,

on the pedestrian street Drottninggatan in central Stockholm. The intensive international cooperation and exchange of information between security services is increasing. Information exchange based on electronic traces, i.e. communications and location data, is essential to this work. Such data has, for example, made it possible to establish how certain Swedish individuals were linked to a number of large-scale terrorist attacks recently carried out across Europe. Also, as public attention has been drawn to matters concerning counter-intelligence and deficient protective security measures at government agencies and companies, the activities of foreign powers against Sweden have been brought more into focus. This should be taken into consideration when assessing the possible scope for changes to the regulation of the obligation to retain data. Also, we have noted a lack of an expressed line of reasoning from the inquiry chair as to the scope of the data retention obligation in relation to the national security of Sweden.

A closer examination of the contents of the proposal

Who communicated with whom?

The inquiry chair proposes that information on *who* communicated with whom no longer be retained in respect to fixed telephony (including fixed IP telephony) and messaging via a fixed network connection point (e.g. from a stationary computer).

Data concerning who was in contact with whom is fundamental to law enforcement agencies' and security services' efforts to gather information about crime, irrespective of whether this pertains to criminal investigations or intelligence activities and irrespective of the methods of communication used. If this data is not available, the risk is great that certain circumstances would go undetected, which would weaken the subsequent analysis and assessment. Nor would there be any reason in many cases to request other communications and location data from the operators, since working with this data would be meaningless.

As opposed to traditional fixed telephony, fixed IP telephony will not be defunct in a few years' time. The Swedish Security Service wishes to emphasise that fixed IP telephony is a modern service which is essentially comparable to mobile telephony. Due to technological advancements, all telephony will eventually be IP-based and thus

mobile in many respects. One and the same IP telephony subscription can be used with both a fixed phone and a mobile phone.

The distinction between fixed and mobile network connection points will also likely disappear or become less clear, making it difficult to determine which one has been used. As optical fibre connections are increasingly used in both home and company contexts, making it possible to use the same IP telephony service both at home and at work, it can already be seen that it is becoming less and less possible to associate services such as telephony to geographical places and physical equipment. The loss of information in a crime-fighting context would therefore be great if the obligation to retain data did not encompass the most modern type of telephony.

This is one reason why crime-fighting efforts would be negatively affected if a differentiation were made between fixed and mobile telephony or fixed and mobile network connections. It is difficult to predict the possible consequences of such a differentiation, especially in an area such as electronic communications with rapid technological advances.

It can at first sight appear as though removing the obligation to retain data for e.g. fixed telephony as compared to that for other data would not have a particularly negative effect on crime-fighting efforts. However, it must be stressed here that fixed phones are not infrequently used for espionage and terrorist activities. Data associated with fixed telephony is still strictly necessary in investigative work. The implications of restricting the obligation to retain data could therefore be very serious. It can at least be assumed that abolishing the data retention obligation would be noticed by capable actors, who would take advantage of this limitation to Sweden's ability to detect, prevent, avert, investigate and prosecute crime against the national security of Sweden. It would likely become much more difficult to gain access to historical data in order to identify the agents with whom intelligence officers are in contact.

Finally, we agree with the inquiry chair's proposal that equipment identities, regarded as subscription data, continue to be retained in regards to mobile telephony. IMEI numbers and MAC addresses are very important in identifying the hardware that has been used in instances of communication. This data provides information on who is communicating with whom, just as the caller's and recipient's number do.

When did the communication take place?

The inquiry chair proposes that data on *when* communication occurred no longer be retained in respect to fixed telephony (including fixed IP telephony) and messaging via fixed network connections (e.g. from stationary computers).

Information on who communicated with whom is, as already pointed out, essential in a law enforcement and intelligence context, but knowing this is of little use if there is no possibility of establishing when contacts occurred in the absence of date and traceable times for when communication started and ended or when messages were sent and received.

It is often of vital importance to know the exact time at which communication occurred. This data is essential in obtaining as complete a picture as possible of a person's contacts, relationships and conduct. This data can also indicate how closely connected individuals are and how they react to various incidents.

The Swedish Security Service collects information on certain individuals who are often very skilled at concealing criminal activities. For example, spies and terrorists sometimes use particular call patterns when communicating. A missed (unanswered) call could indicate one thing, while ringing up twice in a row plus a short call could mean something else, and so on. A short or missed call could be a sign to switch to another mode of communication, a long call could be an indication of a close relationship, a call made at a certain time could indicate that there is an accomplice, etc. Without this type of data, it would be much more difficult to form assessments and the Swedish Security Service could lose its ability to assess the intent and capability of spies and terrorists.

In order to effectively form the most complete picture possible for the purposes of Sweden's national security efforts, access to detailed time records for contacts using all means of communication is necessary. This information is strictly necessary to both criminal and intelligence investigations, and restricting the obligation to retain data could therefore have very serious consequences.

Some general comments on cases concerning electronic attacks should also be given here. Data on the times an actor was online can be considered together with times that electronic attacks occurred, and this data is important for forming a picture that is sufficiently complete to prevent, avert, investigate and prosecute electronic attacks that have a bearing on national security. Cyber threats is a prioritised area and

information on e.g. traceable times is strictly necessary in order to combat this type of crime.

Where did the communication take place?

The inquiry chair proposes that information on *where* communication took place, i.e. location data, no longer be retained in respect to fixed telephony (including fixed IP telephony) and messaging via fixed network connections (e.g. from stationary computers). Because the inquiry chair also proposes that callers' and recipients' IP addresses no longer be retained, this means that data on where communication took place would also be inaccessible for mobile IP telephony and messaging (e.g. SMS, MMS and email messages) via mobile internet connections.

Data on equipment locations during communication is also essential in a crime-fighting context. Such data is often of vital importance in both investigations and intelligence activities and can in certain cases be more valuable than data on who the parties in instances of communication are. Removing the possibility for the Swedish Security Service to pinpoint the location of an individual at a given point in time could in many cases have a serious impact on efforts to combat crimes that have a bearing on national security. This would make it more difficult to counter espionage and terrorism by e.g. pinpointing crime scenes, perpetrators, safehouses, weapons caches, test explosion sites, etc. It would no longer be possible to trace movements made by an individual over time to plan, reconnoitre, meet accomplices or accessories, carry out a crime, go into hiding, etc. Having to rely on cell tower dumps is not sufficient as the exact geographical area is often not known.

The movement patterns of intelligence officers and their agents is essential information for counter-intelligence investigations, which feature capable actors. In many cases, location data is the only way the Swedish Security Service can link individuals to a certain place at a given time. If no such data were retained, this would render the Service essentially helpless in this respect, and have a huge negative impact on the Service's work to counter intelligence activities carried out by foreign powers in Sweden. The Service's counter-intelligence function has described the potential consequences of this as virtually unforeseeable.

The Security Service very frequently receives information in counter-terrorism investigations about a certain phone number, etc. in Sweden and that the person using this selector intends to carry out an

attack in Sweden or another country together with other unknown actors. Such cases are often time-critical and, if the Security Service is not given access to historical communications and location data in order to pinpoint locations and contacts, there is a great risk that suspected threats cannot be assessed and reduced.

Location data is therefore strictly necessary for both criminal and intelligence investigations. In Ministry Publication Series 2014:23 (p. 52) it is stated that the Police have assessed this data to be of extreme importance. We agree with this. Restricting the data retention obligation in this respect could have very serious consequences.

For the sake of clarity, it must also be mentioned that location data at the end of a communication is often equally important as data related to the start of a communication. The inquiry chair has also included this in the proposal concerning telephony via mobile network connections. If information concerning the end of a communication is no longer retained, spies and terrorists will implement a modus of initiating communication with other offenders and keeping the call connected while they are e.g. reconnoitring, monitoring potential victims, travelling, having meetings or taking part in other clandestine activities – all with a view to avoiding revealing information about their location while they are carrying out crimes or crime-related activities.

Information on what type of internet access capacity the individual is subscribing to (e.g. fibre, xDSL, GPRS, UMTS) is also of fundamental importance in this context, as such information makes it possible to indirectly obtain location information. Because the inquiry chair proposes that such data no longer be encompassed by the data retention obligation (see below), the ability to counter crime would be negatively affected.

How did the communication take place?

The inquiry chair proposes that information on *how* communication took place no longer be retained in respect to fixed telephony (including fixed IP telephony) and messaging via fixed network connections (e.g. from stationary computers). How communication took place could regard e.g. whether it was spoken, whether an email account was involved, whether the communication was redirected, whether more than one operator was used, whether the subscription includes voicemail or whether calls have been left unanswered. The inquiry chair also proposes that data on internet access capacity no longer be retained.

Individuals involved in the type of criminality the Swedish Security Service combats often forward communication to other addresses. Forwarding calls from a fixed phone to a mobile phone or similar is easy and could be done in order to conceal crime-related activity. In this respect, the major drawback of removing the data retention obligation would be the elimination of the possibility of tracing calls that are redirected to mobile phones. All the information concerning communication would be "laundered" through fixed phones. This would have an enormous negative impact on efforts to trace the numbers actually used in communication, and enable criminals to escape justice by using fixed phones as bridges in order to remove traceability in the chain of communication. In other words, this would open up the possibility to easily conceal the recipients of calls.

Foreign powers carrying out unlawful intelligence activities in Sweden often use particular call patterns (see above) instead of normal calls. One possible method is call forwarding. Forwarding could also be used to conceal one's location at a certain time. Also, perpetrators quite often shut off their phones before engaging in crime-related activities. Any calls are then redirected to another individual or to voicemail in order to cover up how the mobile phone is actually being used.

Another service that is important to obtain information about is whether there is a voicemail subscription and, if so, when this has been connected. Voicemail content is not encompassed by the obligation to retain data, but this information is important in order to determine whether or not the matter will be pursued further by e.g. seeking permission to intercept communications.

It is of fundamental importance to the Swedish Security Service to know what type of internet access capacity individuals are subscribing to (e.g. fibre, xDSL, GPRS, UMTS). This provides information on whether the connection is fixed or mobile which can, in turn, provide clues as to location. As the inquiry also proposes a decrease in the obligation to retain location data (see above), the negative effect of the removal of the obligation to retain data on how communication took place would be compounded. Data on how communication took place could also provide information on who the subscriber is. Such data is also needed in order to determine which technological solutions to use in interception of electronic communications. Information on internet access capacity is of great importance when determining this.

Removing the data retention obligation would make it much more difficult to identify foreign threat actors operating in Sweden. Spies' and terrorists' ability to communicate clandestinely would increase. The Swedish Security Service can state with certainty that the possibilities

presented by this removal would be taken advantage of by spies and terrorists involved in crime related to the national security of Sweden. This information is therefore strictly necessary for both criminal and intelligence investigations. Restricting the data retention obligation in this respect could have very serious consequences.

Retention period

The inquiry chair's proposal involves differentiating the retention period based on how old data is needed. He proposes that location data for calls be retained for two months. He also proposes that data concerning internet access (except for data identifying the equipment where communication is finally separated to the subscriber) be retained for ten months, and other data be retained for six months.

We have no objection to having a principle of differentiating retention periods but would like to point out that the inquiry chair's reasoning has not taken the Swedish Security Service into account.

The particular nature of criminal activities against national security (such as espionage and terrorism) must be taken into account, as such activities often occur over very long periods of time.

It can take several years for a foreign power to recruit an agent with access to critical information. Such recruitment occurs over an extended period and consists of several stages: analysis, targeting, study, approach, cultivation, recruitment, and gathering of classified information.

Terrorism as well tends to occur over an extended period of time and feature criminal activities carried out in groups. It can take a long time for an individual to develop into an ideologically motivated actor with a terrorist intent and to acquire the capability (knowledge and equipment) to plan and carry out criminal acts.

It is often not possible to predict what communications and location data will be required when the Swedish Security Service first starts gathering information. The inquiry chair states that there is no great need in intelligence investigations for data that is older than five months. As the inquiry chair indicates, this does not apply to the Swedish Security Service. The inquiry into communications data mentioned e.g. that terrorism is a type of crime where data older than two years is needed (SOU 2007:76 p. 173 ff.).

We agree with the inquiry chair's proposal that the retention period for certain data be extended from six to ten months. However,

considering the national security of Sweden, we regard with concern reducing the retention period for location data from six to two months.

We have described above how fundamental we consider data on where communication took place to be to the work of our Service. This information is strictly necessary for both criminal and intelligence investigations. Restricting the data retention obligation in this respect could have very serious consequences. If the inquiry chair's proposal were to be implemented, there would not only be a decrease in the retention obligation for location data but also a reduced retention period. We disagree with this.