Balancing the interests in the context of data retention (INVODAS)

Belgium

Dr. David Stevens (ICRI – K.U.Leuven)

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark*: If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

No, the provisions of the Directive have not yet been transposed into national law, although drafts are being discussed since medio 2008. In order to fully implement the Directive into national law, the basic act on electronic communications (act of June 13th 2005), more precisely its article 126 needs to be amended in order to create a sufficient legal basis for secondary legislation. Although recently (act of February, 4th 2010), the relevant article of the act of June 13th 2005 was amended in order to enable it to serve as legal basis for access to the retained data by national intelligence and security services, the modifications necessary to implement the Directive were not included. The current situation is therefore that the obligations

for operators to collaborate with police and justice services (pre-dating the directive) are still in place (Royal decree January 9th 2003), even though from a strictly legal point of view the legal basis (i.e. old article 109ter, E, § 2, act of March 21st 1991) for these obligations was abolished in 2005.

The following provides an overview of the most relevant stages up to now:

- 2007-2008: preparation of a draft act and secondary decrees by the Belgian Institute for Postal Services and Telecommunications (www.bipt.be)

- May 27th 2008: start of public consultation by BIPT (as requested by telecommunications minister) about the original BIPT-draft

- July 2nd and September 3rd 2008: Privacycommission gives negative advice about the original BIPT-drafts, because too privacy-intruding

- 2008-2009: reworking of drafts, leading to revised texts

- July 1st 2009: positive advice of Privacycommission, under the condition that the draft texts are amended as required by the Commission; on February 2nd 2010, the Commission published an analysis to which extent its required amendments were taken into account; the report indicates that the amended draft act largely corresponds to the requirements.

- October 2nd 2009: minister for the economy and minister of justice requested from BIPT additional advice or report about the costs of data retention obligation for operators

- Early 2010: discussions in Parliament about revised draft, planned to lead to conclusions by April 26th 2010

- April 26th 2010: federal government resigned because of political tensions and thereby limited to "current affairs"

- April 29th 2010: start of the second public consultation organised by BIPT (as again requested by telecommunications minister);

- May 19th 2010: information meeting at BIPT about consultation

- October 1st 2010: conclusions of the consultation on practical implementation of data retention directive published on the website of the BIPT.

Most of these documents can be access though the website of an action group, http://bewaarjeprivacy.be/nl/content/officiele-documenten-belgie. The latest official version of the text was included in the consultation of the BIPT of April 17nd 2008 (http://www.bipt.be/GetDocument.aspx?forObjectID=2808&lang=nl). Later versions of the text (of August 27, 2009) are not yet public, although a version of the reworked draft act circulated (see attachment).

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

The delays mainly have four different reasons, which we would qualify as (1) administrative delays, (2) resistance from telecommunications operators and internet service providers, (3) resistance from the public opinion and human rights organisations, and (4) political instability.

As most important administrative delays, we consider the fact that the originally proposed draft of the BIPT (medio 2008) was unreasonably strict, by imposing many retention obligations not foreseen by the Directive, and by imposing a very long retention period (up to 24 months). These problems were also raised by the Privacycommission in its negative advices on this text (dating July 2nd 2008 and September 3rd 2008).

Further, it seems fair to state that additional delays were caused by the obstruction techniques of telecommunications operators and internet service providers. They were all of course not keen on having extra retention obligations imposed on them, without being sure that they would be sufficiently compensated for retaining extra data. The concerns of the telecommunications operators were also echoed by the telecommunications minister, therefore asking the BIPT to organise public consultations on the respective drafts and/or report on the actual costs related to the data retention obligation.

Further, the resistance of the public opinion (e.g. www.bewaarjeprivacy.be, a website set up by an organisation of telecommunications and internet users) has also not speeded up the adoption of the framework implementing the data retention Directive. Privacy activists and human rights organisations considered the very wide data retention obligations as foreseen in the original draft as a completely disproportionate invasion of the personal sphere.

Finally, it is clear the existing political instability at the federal level is also causing delays, also today since the powers of the government are limited to "current affairs" already since the end of April 2010.

3. Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?

Yes, transposition is certainly intended and quasi-final versions of the texts exist. However, we remind about the fact that the final, official act and decree are still not adopted, so all information given may change in due course.

Regarding possible timing, it seems unlikely that the current government (given its limited powers) will be able to finalise the text and send it to parliament for adoption. Taking into account the current political instability, it is of course difficult

to make projections on when the transposition process could be finalised. Even when a new government would be formed soon, the parliamentary adoption of the drafts will take *at least* another half year (or more).

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   Not applicable.

- ***If transposition has been <u>accomplished</u>:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   No. Belgian legislation is only official in Dutch and French, although basic acts are also (sometimes partially) translated into German.

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   Not applicable for the drafts implementing the Directive. The existing Royal decree of January 9th 2003 contains a basic regulatory framework on the collaboration of telecommunications operators with the law enforcement authorities (including tariffs). This collaboration obligation also lead to a very limited number of retention obligations imposed on operators of public fixed and mobile telecommunications networks or services (so not on internet service providers).

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

      According to the existing Belgian constitution, legislative tradition and practice, the main principles of legislation have to be in an act approved by parliament. Further technical or organisational issues can be left to Royal decrees, which are

in fact made up by the government and signed by the King. The relevant act has to contain the legal basis for or delegation of powers to the King. In relation to the duration of the retention obligation, the (original) law for example stipulated that the period had to be between 6 and 24 months and it was left to the King to decide. From a legality perspective, the privacycommission raised concerns about this broad delegation to the King and asked for more precise rules to be incorporated in the act itself.

Today, there exist drafts of three different texts. One act ("Voorontwerp van wet tot wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering") will amend the existing article 126 of the basic electronic communications act in order to serve as a legal basis for secondary legislation, i.c. two Royal decrees of which the first one will contain the practical aspects and modalities regarding the obligation to retain of data ("Ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van bewaring van die gegevens"), and the second one will contain the further rules about the obligation imposed on operators to collaborate with law enforcement authorities ("Ontwerp van koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie").

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?**

The provisions on data retention will be included in the act on electronic communications. Although a number of extra definitions will certainly be necessary, the basic concepts and definitions will be those already in the electronic communications act, implementing the broader EU regulatory framework on electronic communications. Interesting to note is that according to the latest versions of the texts, there will be no extra definitions added to the communications act, but only to the Royal decrees.

In the data retention decree, the definitions of 'data', 'user', 'telephone service' and 'user-id' are not taken over in the draft decree. By contrast, the draft defines 'personal data' as *"the name(s) of the user, the invoicing and delivery address of the subscriber or the registered user".* The other definitions of the Directive ('cell ID' and 'unsuccessful call attempt') are taken over more closely by the draft decree.

The decree on collaboration with enforcement authorities contains three extra definitions, of the concepts "real time", the service "NTSU-CTIF (National

Technical Support Unit – Central Technical Interception Facility)" and of the "internet sector".

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

As indicated above, the original draft act of 2008 proposed by the BIPT required the retention of much more data than is required by the Directive. Because of the extremely negative advice of the privacycommission a second draft trimmed down the amount of data to be retained. However, also the revised draft requires operators to retain more data than the Directive, including on unsuccessful call attempts.

The recitals to the revised draft law contain an explicit overview of the extra data (going beyond the obligations mentioned in the Directive) to be retained. For the *fixed and mobile telephony service*, the decree also asks to keep some additional identification data: the start date of the subscription, (when applicable) the previous operator of the customer; the extra services to which the user is subscribed and the type (e.g. ATM, credit card, wired money), the identification (e.g. account number, credit card number) and the moment of payments made. For the *mobile telephony service*, the draft decree also requires for the location of the network termination point (NTP) at the end of each connection.

For the *internet access service*, a number of extra identification data are required, such as 1° date and time of subscription or registration of the user; 2° IP-address used for subscription or registration of the user; 3° identification of NTP used for subscription or (when available) registration of the user; 4° extra services to which the user is subscribed; 5° the type, identification en moment of payments. Regarding extra traffic and location data, the decree mentions: 1° the volume of data which were uploaded and downloaded during a session or a specific period of time; 2° the localisation of the NTP at the start and end of every connection; 3° (when applicable) geographic localisation data by means of the cell-ID.

Finally, the following extra identification data are also required for the e-mailservice and internettelephony service: 1° date and time of creation of the e-mailaccount or account for internettelephony; 2° the IP-address which served for the creation of the e-mailaccount or account for internettelephony; 3° the type, identification and moment of payments of the last 24 months.

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

The current legal framework only contains provisions on the obligation of operators for fixed voice telephony, mobile telephony, paging and internet access to collaborate with authorities in criminal procedures. There is no explicit legal basis for an obligation to retain these data, but it is considered necessary in order to be able to comply with the obligation to collaborate. The Royal Decree of January 9th 2003 lists the terms and modalities that have to be complied with when judicial authorities are requesting data in the course of a criminal procedure.

The most important aspects of the obligation to collaborate are:

1. Art. 2: the obligation to install a "coordination cell justice" (operator's single point of contact for receiving requests to collaborate);

2. Art. 3: the obligation to answer requests for identification of subscribers or regular users of a telephone service (cf. art. 46bis criminal procedure code) 'in real time';

3. Art. 4: the obligation to answer requests for the registration of telephone numbers and localisation of telephone calls (cf. art. 88bis criminal procedure code) in real time **until 30 days after the communication**; other requests (i.e. older than 30 days should be answered "whenever the information is available and at the latest during the next working day")

4. Art. 5: the obligation to collaborate in tapping phone communications immediate and in real time (cf. art. 90ter criminal procedure code);

5. Art. 6: general criteria to be met in case of registration of telephone numbers and localisation of telephone calls and/or in case of tapping phone communications, such as:

    a. Geographic issues: being able to send information for the whole coverage area of the operator

    b. Sending of data and content of communications

    c. Sending in generally readable format of data

    d. Sending in clear language when coding, compression or encryption was applied by the operator

    e. Sending data in a secure way; avoiding unlawful interception;

    f. Technical standard that have to be met, such as:

i. ES 201 158 B V1.1.2. (1998-05)

ii. ES 201-671 B V2.1.1. (2001-09)

iii. technical report ETR 331

iv. technical report ETR 232 Rv

6. Art. 10: reimbursement of costs incurred by operators (see also annex).

Further, according to the draft act the Ombudsman for Telecommunications should have the possibility to access similar (retained) data in the context of his powers to fight malicious calls. The same is also applicable in the area of false emergency calls. Further, operators are according to the general privacy provisions in electronic communications also allowed to retain data for invoicing and the delivery of extra services.

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

The draft act (article 3) mentions three different general objectives retention can aim at. Nor the act, nor the decree further limit down the retention of specific data to specific objectives.

1. the investigation and prosecution of criminal offences (according to the existing criminal law procedures);

2. the combating of false emergency calls;

3. the combating of malicious calls by the Ombudsman for telecommunications.

12. Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

No, the draft act does not contain an explicit prohibition or specific categories of data in this respect, but it does provide that the general data protection law remains applicable. Although according to the general data protection law, some specific categories of data are particularly protected than others (e.g. medical data, religion, …), other specific protection regimes (e.g. protection of privacy in electronic communications, criminal procedure law, …) at least at the formal level do not distinguish between different categories of data.

This is without prejudice to the fact that professional organisations dealing with such sensitive data (see question 45) have uttered an interest to introduce these rules into the laws about data retention hat are currently being discussed. Similar concerns also characterised the debate about access of intelligence services to these data.Further, the decree does explicitly mention that data based on which the content of the communication could be reconstructed cannot be retained (article 9 decree).

Finally, some associations of journalists, lawyers and medical doctors have indicated their concerns about the conflict with their fundamental rights, but since the act and decree have not yet been formally adopted, no official steps have been taken to have these rights confirmed (e.g. by cases before the regular courts or the Constitutional Court).

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

As a general rule, the draft act specifies that the retention period is 12 months. After that period, the data should be immediately erased, but exceptions can exist (e.g. accounting or evidence rules). In exceptional circumstances, the King can impose a retention period which can even be longer than 24 months. However, when extending beyond 24 months, the minister for telecommunications is obliged to inform the European Commission.

The data retention decree than specifies from what moment in time the 12 month period starts. For the identification data (both for fixed and mobile telephony, internet access and e-mail and internet-telephony), the period runs throughout the whole duration of the subscription, and up to 12 months after the last registered communication, while the traffic and location data should be kept for 12 months after the communication.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

As indicated above, the retained data will be accessible for law enforcement authorities (judicial police, federal police, investigation judge, public prosecutor), national intelligence and security services, the emergency services and the BIPT and the Ombudsman for telecommunications.

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

The act provides three different purposes for which the retained data can be used: law enforcement (limited to serious crimes only) and the protection of national security, also through the access of intelligence services, the combat against false emergency calls and the combat against malicious calls (through the intervention of the Ombudsman for Telecommunications). The current text and new draft do not grant any specific right to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address.

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

For the law enforcement objective, the rules on data retention are "incorporated" into the general criminal procedure legislation. According to that legislation, there is a "cascade" of possible investigation matters, guaranteeing that the more privacy-invading measures can only be applied in case of sufficient presumptive evidence of serious crimes, such as terrorism, car- and homejacking, armed robbery. Further, the access to retained data can also be allowed for prosecuting specific forms of on-line criminality, such as the distribution of child pornography, organised fraud through the internet or attacks against the communications networks themselves. The issue of access to the retained data for other purposes is much less strictly regulated.

17. **Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?**

The draft data retention act and decree do not mention the need to obtain a specific court order before accessing the data retained, but in the case of law enforcement, the normal criminal procedure applies. According to these provisions, the more privacy-intruding mechanisms or measures (e.g. number registration and tapping, art. 88bis and art. 90ter criminal procedure code) can only be decided upon by an (independent) investigation judge, while less privacy intrusive measure (e.g. identification of subscriber, art. 46bis criminal procedure code) could be decided upon by the public prosecutor. Subsidiarity and proportionality are the main principles in this respect, but the aggrieved party should not be heard or involved in the proceedings before the data is accessed.

18. **Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?**

    Notification of data access is not explicitly foreseen, but it provides that the general data protection law is applicable. Accordingly, the operators are obliged to comply with the provisions of that act (e.g. relating to quality of the data, obligations with respect to the person responsible for processing them, and the rights of the concerned individual (e.g. right to be informed of retention of data). The precise application of these conflicting principles (criminal investigation vs. privacy protection) is however unclear and will depend on jurisprudence.

19. **Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?**

    This possibility for the aggrieved party or obligation for the operators is not explicitly foreseen by the draft act, but it provides that the general data protection law is applicable. Accordingly, the operators are obliged to comply with the provisions of that act (e.g. relating to quality of the data, obligations with respect to the person responsible for processing them, and the rights of the concerned individual (e.g. right to be informed of retention of data). The precise application of these conflicting principles (criminal investigation vs. privacy protection) is however unclear and will depend on jurisprudence.

20. **May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?**

    Recourse to a courts or specific remedies are not explicitly foreseen in the draft act, but follows from the existing provisions of civil and criminal procedure law. An eventual unlawful data access could in first instance be considered as a breach of the data protection law and be administratively investigated and sanctioned by the privacycommission.

21. **Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.**

    Yes, in this respect the draft act defines a new criminal offence. Accessing or using of the retained data for other purposes than those identified in the act is punished with fines up to 275k€ and imprisonment up to 3 years (article 4 draft act).

22. **When do the accessing bodies have to destroy the data transmitted to them?**

    The draft act or decree do not contain specific provisions in this respect.

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

The provisions on data retention apply to four different categories of operators: 1° operators of a public fixed telephony service; 2° operators of a public mobile telephony service; 3° operators of a public internet access service; 4° operators of a public e-mailservice or a public internet telephony service. Operators that offer different services are required to retain all the data of the different services they offer. By extending data retention obligations to the operators of e-mailservices and/or internet-telephony services, the draft act and decree already stretch the scope of the retention obligations beyond the scope of the general electronic communications act. While the original draft also seemed to apply to private networks, it is now clear that this is no longer the case. Moreover, retention obligations are for obvious reasons also not applicable to the operators of networks, but only to the providers of services over those networks.

Finally, we should refer to the recent judgement of the Court of Appeal of Gent in the "Yahoo"-case, in which the Court explicitly mentioned that according to the current legal and regulatory framework the internet service or webmail provider Yahoo was not to be considered as an "operator" of an electronic communications network or provider of an electronic communications service (full-text: http://www.timelex.eu/userfiles/files/pub2010/20100630_Gent%20-%20OM-Yahoo.pdf).

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

The draft act and decree do not contain exceptions in this respect, although the idea has been discussed.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

Although the legal basis (old article 109ter, E, § 2, act of March 21st 1991) of it has been abolished by the act of June 13, 2005), it is generally accepted that the Royal decree of January 9th 2003 is still largely valid. This decree is also still applied in practice by most operators. According to it, operators have to collaborate with the law enforcement authorities. Besides the obligation to be able to deliver the law enforcement authorities some data in real time, the decree also states that operators have to retain some communications and localisation data for a period of at least 30 days in order to be able to contribute to a number registration procedure.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

Yes, the draft act stipulates that the general data protection law is applicable, which of course results in a number of additional rights for the citizens (e.g. right to access and correction, although the precise impact of these conflicting norms is unclear), and also a number of additional general data protection related obligations for the telecommunications operators (e.g. obligations on data quality and protection against unlawful intrusion).

27. Which *additional* costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

In its document summarizing the results of the consultation on the practical aspects of the organisation of the obligation to retain data, the BIPT refers to the estimations of larger operators that the (additional) costs to meet the requirements of the data retention obligation could represent between 0,5 and 5 million euro (expected additional needed storage capacity of between 2 and 15 Tbyte). These estimations are however not really sufficiently demonstrated by hard figures during the consultation. The BIPT therefore concluded it cannot yet determine the precise additional cost or price for the foreseen additional retention obligations. Of course, as long as the precise modalities are not fixed by law , the final costs cannot be calculated precisely.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

The operators themselves should carry the costs for the investment, exploitation and maintenance of the technical means needed in order to comply with the data retention provisions at their side, while the ministry of Justice should carry these costs for the judicial authorities. However, the Royal decree does foresee the principle that the operators will receive a specific reimbursement for their actual collaboration, but the amount is not fixed yet. In its most recent consultation, the BIPT is suggesting that the reimbursement fees are too high (also compared to a number of surrounding countries). The BIPT therefore plans to hire another consultant in order to establish a cost-model for the price of data retention products.

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

As it is already the case for the current data retention and collaboration procedures, the draft decree foresees a specific instrument of collaboration, called the "coordination cell Justice". Every operator has to assign one or more contact persons among its personnel which shall be responsible for the retention of data and should also be permanently available. The decree than specifies a number of requirements these persons have to comply with (e.g. specific professional qualifications). The decree also explicitly mentions the possibility for operators to create a "shared coordination cell" in order to reduce the costs. The "coordination cell Justice" will then be responsible for delivering the requested information to the BIPT (telecom regulator), which hands it over to the relevant judiciary authorities.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

Yes, the draft act creates a new criminal offence, potentially leading to a fine of up to 275k€ or 3 year of imprisonment. Any person that, with the intention to cause damage or to commit fraud, copies, keeps or uses the data which he has got access to via the official procedures and that is not complying with the procedures mentioned in the act will be subject to the mentioned fine or imprisonment. The same applies for any later persons that (knowingly) would get access to data collected under these circumstances. The draft act does not explicitly mention the possibility of compensation of damages, but this follows from the principles of general civil and administrative law.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

According to the draft act, the BIPT (i.e. telecommunications regulatory authority) will serve as an interface between the party retaining the data and the party requesting access to the data.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

No, justice and privacy in electronic communications are mainly federal competences. Access to the retained data is limited to the cases of 1° criminal procedure (i.e. access by federal officer of judicial police in exceptional cases, access by public prosecutor for less privacy intrusive measures and access by

investigation judge for more privacy intrusive measures; 2° protection of the integrity of the state (i.e. access by intelligence services); 3° combat against malicious calls to emergency services (i.e. access by emergency services and BIPT); and 4° combat against malicious calls to private users (i.e. access by the Ombudsdienst).

33. **What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?**

    During its most recent consultation (April 2010) the BIPT clearly indicated the intention to streamline the access procedure, in order to avoid mistakes or breaches of confidentiality. Therefore, the BIPT asks the market players about their willingness to create a fully automated, electronic platform for organising the access to the retained data, mainly based on the ETSI-standard TS 102 657. The current situation (with requests originating from more than 5 different sources and each times being sent separately to the relevant operator) would then be replaced by a centralised (one stop shop) ticketing system. Most operators are in favour of a more standardised procedure based on ETSI TS 102 657, and in favour of a Single Point of Contact (SPOC) for all requests of the public authorities.

34. **On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?**

    The draft decree does not contain specific rules on extra-territorial requests. The matter will therefore have to be considered according to the general criminal procedure provisions for establishing rogatory commissions (e.g. requests for assistance of judicial authorities or requests for assistance in collecting proof at the territory of another member-state). The draft act also does not contain any provision for granting access to retained data. According to these provisions, the competent authorities are therefore always the counterparts of the Belgian judicial authorities in other member states.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

The relevant supervisory authorities are the (independent) BIPT (telecom regulator), the (independent) privacycommission, the department of Justice and the manager of the coordination cell Justice (see above). It should be noted that independence of (public) regulatory authorities can - according to the Belgian constitutional framework - never be 'complete'. Government, parliament always remain competent for issuing general policy instructions to the regulatory authorities and for approval of their budgets. The level of independence of regulators is always considered in function of their tasks (e.g. the government can in principle not intervene in the decisions of the regulator s in individual cases) It seems therefore fair to say that both authorities are not "complete independent" from government in the sense of the recent judgement in the German data protection case.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

Not that I'm aware of, although some organisations have threatened to do so when the drafts would be approved. On the interpretation of the current regime (stating that ISP's and/or webmailproviders are not to be considered as electronic communications operators or providers: see also question 23.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

- new data retention regime: n/a
- current regime: Yahoo (webmail provider)

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

- new data retention regime: n/a
- current regime: scope and applicability of electronic communications regulatory framework (incl. data retention) was questioned

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

- new data retention regime: n/a
- current regime: the Court of Appeal ruled that ISP's and/or webmailproviders as Yahoo are not to be considered as electronic communications operators or providers

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

Not that I'm aware of.

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

The practical aspects and modalities of the new retention obligations are not finally decided upon. In the current system, each "side" has to take care of its own investments (e.g. operators vs. law enforcement authorities, see art. 10 decree January 9th 2003).

As indicated (see question 10), the current situation is quite unstable for a number of reasons: 1° the legal basis of the decree has been abolished; 2° the obligation to retain data is not explicitly stated, but deduced from the fact that operators are obliged to collaborate on certain data point with judicial authorities; 3° the fact that the obligations mentioned in the decree were formulated as a temporary solution. In practice, article 7 mentions the following information to be provided by operators in case of a collaboration request for the registration of telephone numbers and/or the localisation of telephone calls(art. 88bis):

a. telephone number of incoming calls
b. telephone number of outgoing calls
c. precise date and moment of telephone call
d. precise beginning and ending of the call
e. type of communication (i.e. incoming, outgoing or diverted call

f. for mobile services: cell identification information (mobile telephony) or coordinates of satellite base station (satellite telephony).

Providers of internet access are according to this provision required to be able to deliver the follow data:

a. assigned IP-address (fixed or temporarily)

b. identification data of the subscriber, and when possible exact location of the connection to the provider of internet access

c. date of the communication

d. beginning, ending and duration of the communication

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

The draft act stipulates that the retained data should be "unlimited accessible" from within the territory of Belgium. Further, the draft decree provides that the "coordination cell Justice" (i.e. the person(s) the public authority can contact with its request of access) should be localised inside the Belgian territory. The precise interpretation of this requirement is however still unclear, although it seems to pre-suppose that data can also be stored abroad. The minimum guarantee the draft act requires is indeed that it can be accessed from within Belgium. At least the act does not contain an explicit obligation to store in the Belgian territory.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

Most important in this respect are the requirements as they follow from the application of the data protection legislation (see question 19). Further, the act provides different reporting tools (e.g. yearly report to EU Commission and national parliament by relevant ministers, but also reporting from operators to minister, via BIPT), and the obligation to evaluate the functioning of the data retention provisions. Besides the general provisions on security, protection, technical and organisational measures, the draft decree also foresees specific requirements for the persons which serve as "coordination cell Justice". For an overview of these requirements, see article 11 of the draft decree, requiring i.a.:

- processing and handling of requests in full independence;
- access to all data and to the offices of the operators;
- protection against (random) dismissal by the employer;

- appropriate level inside the undertaking in order to guarantee direct reporting to management and/or data controller;

- specification of the task of the coordination cell (e.g. assure compliancy with act, with specific data for specific purposes, with rules on authorized access to the data, and with protection of the retained data);

- copies of advices and report of coordination cell need to be sent to the privacycommission;

- finally, some personal information about the person responsible for the coordination cell needs to be provided to the privacycommission (e.g. identification and contact data, legal relationship with employer, description of office and service; professional qualifications, specific measures taken by the data controller.

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

The draft decree specifies the general requirements the operators have to comply with in a functional way (article 7), stating that: 1° the data need to have the same quality and enjoy the same level of protection as the data in the network; 2° the operator has to take appropriate organisational and technical measures to protect the data against deletion, loss or modification, and against unlawful storage, processing, access or publication; 3° the guarantee that in principle only the coordination cell has access to these data; 4° and (notwithstanding exceptions, such as data needed for facturation or fiscal reasons) the guarantee that data are effectively deleted at the end of the retention period. the draft act also provides that the data should be organised in such a way that they can immediately transmitted to the relevant authority (article 8) and the general rule that data from which the content of a communication could be deduced cannot be retained (article 9).

c) data are not used for purposes other than those they are permitted to be used?

Only general rules, see also answer sub a) and b).

d) **data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.**

Only general rules, see also answer sub a) and b).

e) **data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?**

The draft decree only provides the general obligation and does not specify further precise rules or modalities on this issue.

f) **the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?**

n/a

g) **sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?**

The draft decree only provides the general obligation and does not specify further precise rules or modalities on this issue.

41. **Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?**

Yes, the draft act and decree provide that these concerns are taken into account by the supervision of the BIPT and the privacy commission.

42. **What technical (de facto and/or de iure) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?**

The draft decree specifies standards the operators have to comply with, both as regards the retention of data and the collaboration with law enforcement authorities. Moreover, the BIPT is consulting about the idea to create a centralised system where all operators could contribute to (as we already have it in Belgium for number portability). However, the most recent consultation of the BIPT has showed that this idea is supported by only very few operators. Regarding technical standards to be used, all operators are in favour of implementing and applying ETSI TS 102 657.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

The practical aspects and precise modalities of the exchange have not yet been fixed. In its consultation, the BIPT is looking into a scenario where all the retained data is centralised in a central "coordination cell Justice" and then through a one-stop-shop procedure run by the BIPT forwarded to the relevant and competent authorities requesting access, in accordance with the law on criminal procedure. However, since operators sent in only very few data about the costs of the new data retention obligations, BIPT came to the conclusion that the issue should be studied further, leading to a cost-model for efficient data retention products and a glide-path for lower prices which should start at 31 December 2010.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

The draft decree does not contain specific provisions on this issue, so international collaboration will only be possible through existing criminal law procedures.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

As indicated above, the adoption process has been characterised by significant delays. Moreover, the debate surrounding the issue has in general not been very intense. Some privacy activists and human rights organisations have launched a specific website with a petition, which until now (only) received 4115 signatures. This is most likely one of the consequences of the fact that the issue has largely been presented as a technical debate between telecommunications operators and the law enforcement authorities. Even after the original (very strict) draft as it was proposed by the BIPT, the reactions remained rather limited. In general, the debate about the implementation provisions is mainly taking place between law enforcement authorities and the telecommunications regulator at the one side, and operators at the other side. Further, some human rights organisations have entered the debate, as well as some professional organisations (journalists, lawyers and

medical doctors) and the association of internet providers and service providers (www.ispa.be).

In the first half of 2010, the minister of Justice indicated his intention to finalise the act and decrees, since he was concerned about the fact that Belgium - as president of the European Council in the second half of 2010 - would have to evaluate the implementation of the Directive, not having it implemented in national legislation itself. However, broader political discussions and instability led to the fact that also today, the act and the decrees have not been finally adopted.

46. Are there any obligations in your country to retain other personal data without a *specific* reason (e.g. passenger name records (PNRs), employment data, etc)?

Yes, data retention schemes exist in many other sectors (e.g. obligation to store data for invoicing or accounting purposes, obligation to store data in labour sector, ...). However, I do not feel very well placed to provide a precise overview of these issues in other sectors.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

No, there are very few data easily publicly available. The summary of the most recent consultation contains an overview of the costs for the current collaboration and data retention (mainly related to (fixed or mobile) voice telephony (total cost: 19,5 million euro in 2009). In the context of the discussion on how long the retention period should be, the draft act provides some relevant figures on identification of IP-addresses in 2007:

Réquisitions du parquet fédéral concernant l'identification d'adresses IP en 2007

Age des données demandées	Pourcentage des demandes	Pourcentage cumulé des demandes	Identification positive
Moins de 6 mois	15 %	15 %	
Entre 6 mois et 12 mois	51 %	66 %	76 %
Entre 12 mois et 18 mois	18 %	84 %	76 %
Plus de 18 mois	16 %	100 %	46 %

Données : police judiciaire fédérale, DJF / FCCU

The draft act provides that the effectiveness of the data retention obligation should be evaluated within a period of two years after its entry into force.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

Not that I'm aware of.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

As indicated, after recently having consulted on the practical issues of the organisation of retention and access, the BIPT is now planning to ask a consultant to work out a specific cost-model. Regarding all other issues, the current draft act and decrees are probably quasi-final and there is not a lot of debate on this issue, although the association of internet and services providers (ISPA) is quite actively in following up and lobbying.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[1] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

Belgium is a Western European state and also a member of the European Union. As such, all Belgian citizens enjoy the fundamental rights mentioned above, and in particular those related to the protection of privacy and personal data. Those rights have been incorporated in the Constitution, in article 22 which guarantees the right to respect for the private and family life. The protection of the communications privacy and secrecy is further mainly elaborated in the articles 124-133 of the act on electronic communications. As a basic rule, it is prohibited (and punished as an

[1] In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

criminal offence) to - without the permission of all participants to it - take notice of the *existence* of an electronic communication (i.e. the fact that a certain communication is taking place), or of the *content* of an electronic communication. The act provides a number of exceptions, such as for invoicing purposes, for monitoring the quality of call centres, and for law enforcement purposes.

In the area of data retention and content of electronic communications, it should be noted that the draft royal decree on data retention explicitly mentions the prohibition to retain data which could lead to the possibility to reconstruct the *content* of a communication (article 9).

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The exercising of the fundamental rights in relation to data protection is only possible according to the provisions of the international, European and EU data protection regulatory framework, of which article 22 of the Constitution of the copy at national level.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

n/a

53. Does national (constitutional) law safeguard an *absolute* limit as to the maximum degree to which public surveillance measures *collectively* may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

Although the Constitution most certainly contains an absolute limit as to the maximum degree to which public surveillance measures *collectively* may restrict fundamental rights, the Constitutional Court can only clarify this absolute limit by pronouncing itself in individual cases (in which it can annul unconstitutional legislation). However, since the provisions have not yet been adopted, there are also not yet cases pending before the Court.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

n/a

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated

parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

In discussion with government and the regulator, the market players are expressing their concerns about a possible violation of their fundamental rights, such as the freedom of commerce or the protection of private property. Until now, there is however only very few literature or debate on the issue from this perspective, but I would expect the Constitutional court in any case to come to a balance between these conflicting fundamental rights. Proportionality will be the key criterion used in order to judge such a case. In this respect, the quite broad Belgian retention obligations make the act more vulnerable.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

The draft act and decree only require from private parties a role in the actual retaining of data, not in sending it to the relevant (e.g. law enforcement) authorities. The access to retained data is organised according to (other) existing procedures, such as the criminal procedure code (for the access for judicial objectives), and the acts on the telecommunications sector (for the objective of combatting malicious calls, access by the emergency services and the Ombudsdienst).

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

The question whether this follows from constitutional principles has not arisen, since under the already existing collaboration obligation imposed on them, the operators are (partially) reimbursed for the costs incurred. If reimbursement would not have been foreseen by law, the principles on the protection of private property would have been most likely to come into consideration as a basis for such right.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

Belgium is a member of the Council of Europe and is therefore obliged to take the ECHR into account. Further, the ECHR is also part of the European regulatory framework through article 6 para. 3 TFEU, so being a Member State of the European Union Belgium also has to guarantee that its legislation take the provisions of the ECHR and the jurisprudence of the Court on Human Rights sufficiently into account.

Since 1971 (ruling of May 27th in the case Franco-Suisse Le Ski), the Highest Court in Belgium (Hof van Cassatie) has been building on a doctrine stating that international rules with direct effect (such as the ECHR) are assigned with a higher position in the 'hierarchy of norms'. In practice, this means that courts and administrations have to leave aside (cannot apply) the national constitution, legislation or secondary legislation which would not comply with these international sources of law with direct effect.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

Yes, based on the doctrine of the direct effect of European directives, citizens can in some cases directly claim rights, although normally European directives have to be transposed into national (or regional) law through parliamentary (and secondary) legislation.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

No, in principle European law takes a higher position on the ladder of hierarchy.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

The data retention regulatory framework has been developed by the ministries of telecommunications and justice, both at federal level. Regional authorities have no relevant competences in this area.

For the organisation of access to retained data and the authorities concerned, see questions 10, 17 and 32.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

This issue is not explicitly mentioned in national (constitutional) law and could therefore only in very exceptional cases (integrity of the state etc, terrorist attacks, …) lead to actual limits in practice.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

Getting the act and decrees adopted will already be a great first step. Further, more public debate about the issue would also be welcome, since now most citizens are not aware of the issues at stake because the debate is often limited to quite technical discussion between the operators of telecommunications services on the one hand, and the law enforcement authorities on the other hand.

Addendum

The most important evolutions in the period between the closing of this report and its publication relate to:

1. Evolutions in the legal framework:

    a) The reasoned opinion of the European Commission of May 30th 2013 (ref. C(2013) 3033 final) for non-transposition of Directive 2002/58/EC (which contains a useful overview of the state of affairs on that date);

    b) The adoption on 30th July 2013 of the Act amending the relevant articles of the Electronic Communications Act of 13th June 2005 and of the Criminal Procedure Code in order to create a solid legal basis for the implementation of Directive 2002/58/EC *("wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering")* and its subsequent publication in the Official Gazette of 23th August 2013.

    c) The adoption of the Royal Decree implementing the Act, expected towards the end of 2013.

2. Evolutions in jurisprudence:

    - The Yahoo-case mentioned on p. 12 of the report (in which operators of webservices were not considered as "operators of electronic communications services or networks") has been annulled by the Highest Court *("Hof van Cassatie")* on January 18th 2011. The case was referred to the Court of Appeal of Brussels, which in its judgment of October 12th 2011 focused mainly on the issue of extra-territoriality and on that ground acquitted Yahoo. This judgment was however again appealed before the Highest Court, which on September 4th 2012 annulled it and referred the case to the Court of Appeal of Antwerp.

3. Evolutions regarding the independence of the BIPT:

    - On June 20, 2013 the European Commission has sent Belgium a reasoned opinion on the independence of the (federal) regulator for telecommunications, the Belgian Institute for Postal Services and Telecommunications (BIPT). The Commission considers that by maintaining the possibility for the government to suspend some decisions of the BIPT and by requiring the approval of the long-term plan of the Council of the BIPT by the Council of Ministers, Belgium has violated the Articles 3 (3a) and 4 of the Framework Directive.

Balancing the interests in the context of data retention (INVODAS)

Belgium

David Stevens

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

No. In Belgium, there is no constitutional or legislative provision which explicitly provides the right to communicate *anonymously*. At constitutional level, article 29 protects the secrecy of (physical) *letters,* but it not clear to what extent the article also protects new forms of correspondence and communications. In the past, some attempts have been made to widen its scope to new (electronic) forms of communication, but no progress has been made so far. Article 22 of the Constitution protects the private and family life of citizens. Since the scope of this provision is not limited as regards the *medium* used, new forms of (electronic) communication are also protected under this article.

At legislative level, two different sets of provisions protect the *secrecy of electronic communications*.

1. By stating that nobody is allowed to perform conflicting acts, without the consent of all other direct or indirect concerned parties, article 124 of the Electronic Communications Act (of June 13th 2005, short: ECA) protects: 1° the existence of information transmitted via electronic means; 2° the identity of the persons involved in the transmission; 3° the transmission data related to other persons; 4° the processing, modifying, deleting or publishing of the protected information, identity or transmission data. Breach of this article is punished with fines up to 275.000 euro by article 145 of the ECA.

2. The Criminal Code also protects the secrecy of private communications and telecommunications during the transfer between the communicating parties by respectively prohibiting the interception of information by public officials or civil servants (art. 259bis CC) and by private persons (art. 314bis CC). Legal

exceptions to this regime are provided by the articles 46bis, 88bis and 90ter through 90decies of the Criminal Procedure Code. These articles contain the procedures for the interception, taking notice, and/or recording of private communications in the context of the investigation of specific criminal offences.

Article 125 of the Act lists a number of exceptions to the application of both these regimes, such as: 1° in case another law explicitly allows or imposes the in principle prohibited acts; 2° in case the prohibited acts are performed only with the intention to guarantee the proper functioning of the network; 3° in case the acts are needed in order to enable emergency services to provide assistance; 4° and 5° in cases the acts are performed by the telecommunications regulatory authority or Ombudsman in the context of carrying out of their tasks; 6° in case the acts are needed in order to avoid end-users receiving unsolicited communications.

Finally, a number of other provisions of the Electronic Communications are relevant in the context of the right to communicate anonymously. First, article 48 of the Act stipulates that the (private) usage of cryptography in electronic communications is free, but that the offering of cryptographic services to the public can be subject to a notification to the telecommunications regulatory authority. Second, the possibility to communicate anonymously is quite seriously limited by article 127 ECA. In its first paragraph, this article enables the government to impose on operators of networks, on providers of services and on end-users the technical and administrative measures in order to be able to identify the calling line in case of emergency calls, as well as other investigatory powers in the context of the prosecution of specific crimes. In its second paragraph, the article states that it the delivery or usage of telecommunication services or equipment are prohibited when they make it impossible or render it more difficult to comply with the obligations mentioned (i.e. contributing to calling line identification, wiretapping, tracking, monitoring or recording of communications). The only exception to this prohibition, is the usage of encryption systems which enable the confidentiality of the communication and the security of payments. As a sanction, paragraphs 4 and 5 state that operators or end-users that not timely comply with these requirements to collaborate will no longer be allowed to offer or receive electronic communications services. Thirdly, article 130 ECA contains specific and detailed rules about the (commercial) service ‘calling line identification’ to which users of fixed and mobile telecommunications can subscribe.

2. **Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?**

As previously indicated, Belgium does not have a real (or enforceable) framework for data retention. Article 126 of the ECA only contains the general obligation to retain data and stipulates that for data about public telephony the retention period should be between 12 and 36 months. This provision has however not yet been executed further by secondary legislation.

Regarding the transposition of the data retention directive, no new real initiatives or improvements have been made since our previous report. The existing act has not yet been modified and secondary legislation therefore also has not yet been approved. The reasons as they were given in answer to question 2 still remain valid (government still in "current affairs"). The Evaluation Report of the European Commission on the Data Retention Directive indicates that the Belgian authorities claimed to already partially have transposed the Directive (cf. Commission Report p. 15 and footnote 16). Most likely the Belgian authorities are referring to the existence of the general article on data retention, as it was already included in the ECA of 2005 (art. 126).

There has been little (public) debate about the transposition of the directive, and the arguments that were put forward did not really change since our previous report ("technical discussion between operators and public authorities").

"Quick freeze" procedures are not considered as formal alternatives to the data retention obligation, but it could nevertheless be argued that the existing (very broad!) obligations for operators to collaborate with police and judiciary (and national intelligence and security services) somehow function as substitute *in practice* and lower the pressure (or urgency) of developing a proper data retention framework.

Since our previous report, two closely related texts were approved:

1. The Royal decree of October 12th, 2010 specifying the modalities of the obligation of operators to cooperate with intelligence and security services in the domain of electronic communications (i.e. the execution of the act of February 4th 2010 regarding intelligence and security services, as mentioned in our previous report).

2. The Royal decree of February 8th, 2011 modifying the existing Royal of January 9th 2003 on the obligation for operators of electronic

communications networks or providers of services to collaborate with police and justice for the prosecution of criminal offences. The three main changes of the Royal decree of 2011 relate to:

- the obligation for operators to have a dedicated 'coordination cell justice' (see art. 3) and other changes to the modalities of the obligation to collaborate (see art. 4 – 7 and 12);
- the objective to lower the costs of the justice department, by lowering the fees paid to the operators by 30% on average (see art. 11 and annex);
- the objective to abolish the exclusion of the internet sector (see art. 13).

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

Operators of electronic communications networks and providers of services are (based on article 127 ECA) required to comply with a number of technical and administrative obligation for the purpose of identifying the calling line in case of emergency calls. They are also obliged to collaborate with police and justice in the pursuit of criminal offences in a number of different ways (e.g. identification of the calling person, tracking, localisation, overhearing and recording of private communications).

On January 18th 2011, the Highest Court ("Hof van Cassatie") annulled the judgement of the Court of Appeal of Ghent of June 30th 2010, in which the court stated that Yahoo! could not be considered as an "operator of an electronic communications network" or as a "provider of electronic communications service" and therefore was not obliged to collaborate with police and judiciary (see question 23 in previous report). The Highest Court ruled that the interpretation to be given to the relevant provisions of the Criminal Procedure Code should not be identical to the interpretation of the provisions of the ECA. By consequence, although Yahoo! potentially could not be qualified as an "operator of an electronic communications network" or as a "provider of electronic communications service" according to the ECA, it nevertheless qualifies as such under the Criminal Procedure Code (art. 46bis, identification of a user).

Further relevant in this respect, are 1° the exceptions to the principle of secrecy of electronic communications as listed in article 125 ECA (see answer to question 1, above), and 2° article 128 ECA, which contains an explicit ground for retaining communication and traffic data with a view of proving a commercial or business transaction, given the parties were informed about this registration. Finally, based on general principles of law, citizens and undertakings are obliged to retain data (potentially including electronic data) in order to serve as proof in civil or fiscal

matters (e.g. undertaking obliged to maintaining copies of their invoices for 10 years).

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

   The prohibition of self-incrimination is a well-established principle of Belgian criminal law, implying that no person can be required to provide proof of his own guiltiness to an offence. Therefore, in case privately retained data could lead to such self-incrimination, the concerned person could most likely not be obliged to deliver this evidence.

   Further, a number of specific professionals (such as doctors, priests, lawyers, …) are protected by a professional secrecy, but the "interface" between this right to secrecy and the obligation to provide evidence falling within the scope of the Data Retention Directive has not yet been an issue of concern, since a national data retention framework is not yet in place. The legislation on national intelligence and security services explicitly mentions that those services should respect the principle of the professional secrecy of certain persons.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

   Regarding the retention of traffic data and identification data of end-users, the current version of article 126 ECA provides the government with a very broad delegation, since it can (after advice of the minister of Justice, the Privacy Commission and the telecommunications regulatory authority) decide on the conditions and modalities of data retention obligations for operators. The only additional requirements imposed by article 126 §2 ECA are: (a) that the retention period for data about public voice telephony should be between 12 and 36 months, and (b) that the retained data should be "unlimitedly accessible" from within the territory of Belgium.

   Further, operators also have to comply with the obligation to collaborate with police and justice on the one hand, and with national intelligence and security services on the other hand. Both sets of legislation require similar approaches regarding the request, storage, security and protection of retained or obtained data. According to the articles 3 and 2 of the respective decrees, the operators should designate a dedicated "coordination cell justice", which is available 24/7. The coordination cell receives requests from the telecommunications regulator. The telecommunications regulator forwards the information received from operators to the department of

Justice or immediately to the national intelligence and security services. The department of Justice is responsible for ensuring that the received information is passed on to requesting judicial authority.

In some specific cases (e.g. identification of calling person, art. 46bis CPC), the entitled authorities (e.g. police service NTSU-CTIF) are allowed to directly access to the customer database of the relevant operator and the decree even allows them to decide on the technical details of this procedure themselves. When doing so, the NTSU-CTIF has to keep a log and a journal of every access to and consultation of the databank. The NTSU-CTIF is also obliged to ensure sufficient physical and software related measures are taken to ensure a proper level of security.

None of the above mentioned decrees contain further specific provisions on the storage or security of the information obtained, but it is argued that the basic principles of the data protection act should also be complied with.

6. Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.

Some statistical information about the obligation of data retention were included in our previous report (see estimation of policy and judiciary, and the report on the BIPT consultation on this issue). Since then, no additional figures have been made public.

The Royal decree on the obligation for operators to collaborate with police and justice indicates that the total cost of telephony is as high as 20% of the total budget of law costs of the justice department (i.e. 19.192.179,95 euro of telephony costs, as part of a total budget of 92.997.618 euro). In order to reduce law costs and because of the lower calculated "real" cost for operators to deliver this data, the Decree on average lowers the compensations for operators with 30%. Further future reductions, based on a cost model drafted by the telecommunications regulator are explicitly not excluded.

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

As the current status and framework on, data retention and similar obligations itself, the judgement on the constitutionality of the data retention regime is highly complex.

First, it has to be recalled that a true data retention framework does not yet exist. The existing legal basis for imposing data retention obligations (art. 126 ECA) predates the data retention directive and has to be replaced in the future in order to be effective. Since it has not yet been executed by secondary legislation, it is not

enforceable on operators. Therefore, they have no incentive to attack the legality or constitutionality of the current regime. However, it seems reasonable to expect that even the current article 126 could be judged unconstitutional by the Constitutional Court, since it is formulated in quite a general and abstract (not to say: vague…) way and delegates important (privacy invading) powers to the government.

Second, as regards the future data retention regime as it is envisaged by the (current) draft acts and decrees (already mentioned in our previous report, see questions 10 and 11), it also seems not unlikely that they would be judged unconstitutional in a case before the Courts. The main arguments for this relate to the fact that the draft texts 1° impose the retention of significantly more data than allowed by the Directive; 2° do not sufficiently specify the purposes for which specific data has to be retained; 3° offers quite limited guarantees in order to make sure the personal life of citizens is not disproportionately invaded (e.g. unclear scope vis-à-vis the EU directive; no prohibition to retain specific sensitive data; broad access to retained data by public authorities).

8. **Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?**

As indicated in our answer to question 1, the secrecy of (electronic) communication is from a constitutional point of view not so much protected by the provisions on the secrecy of (physical, postal) correspondence (art. 29 Constitution), but rather by the provision on the protection of private and family life (art. 22 Constitution). Further, additional provisions on the secrecy of electronic communications exist at legislative level, especially in the Electronic Communications Act of 2005. The protection offered by these provisions is quite broad (existence of a communication, content of communications, transmission data), but nevertheless the act also contains quite generally formulated exceptions in a number of cases (see above, on art. 125 ECA). As an example, we might refer to the exception for the telecommunications regulatory authority, which can *in general terms* perform all acts necessary for fulfilling its (legally defined) inquiry powers.

Because of the wide scope of the protection of the secrecy of electronic communications, it seems likely - at least based on the current draft versions of acts and decrees on data retention - that all data to be retained will be protected as secret.

9. **Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.**

The Constitutional Court recognizes the "principle of proportionality" as a general principle of law, which is *inherent* in the execution of any public power. Applying it the Court can annul any piece of legislation which it considers not in line with the principle of proportionality.

The proportionality of a measure will also be a crucial element in the appreciation of the Constitutional Court when assessing the conformity of a privacy-invading measure with the European and International Treaties (e.g. art. 8 ECHR). As regards its scope of application, it should be noted that the Constitutional Court also accepted that both paragraphs 1 and 2 of art. 8 ECHR are characterised by a "horizontal effect", meaning that also citizens can invoked this article in their mutual relationships.

As indicated in our answer to question 7, the (lack of) proportionality of the envisaged future data retention framework is precisely one of the most likely legal grounds for annulment by the Constitutional Court, since the consequences of the obligation imposed could be judged not to be proportionate to the purpose of the measure. In the past, the Constitutional Court already applied the principle of proportionality in a judgment of 21 December 2004 in which the Constitutional Court declared several provisions of the CPC (e.g. the possibility to perform a "quick house search" without involving a magistrate) unconstitutional.

10. Has transposition of the Directive in Belgium been finalised in the meantime?

- **If so: Please explain in which points the new legislation differs from the draft version referred to in your answers to questions 7 to 35 of the first questionnaire (please reply question by question).**

- **If not: please describe, on the basis of questions 7 to 35 of the first questionnaire, how the legislative procedure and/or the public debate has evolved since the submission of your answers to the first questionnaire. Is transposition still intended? If not: how does the government intend to deal with possible sanctions (in particular, as a consequence of EU infringement proceedings)?**

No, transposition has not yet been finalised. Moreover, no real progress has been made (although some changes were made to the provisions on the obligation to collaborate with police, justice, and national security and intelligence services). The main reasons for the delay also remained unchanged: institutional and political instability at the federal level, government in 'current affairs').

Surprisingly, the federal authority seems to have indicated that it already partially transposed the Directive, this statement can in practice hardly be shared. In fact, the current legal provision for a regulatory framework on data retention (i.e. art. 126 ECA) even predates the adoption of the Directive and has not yet been executed by secondary legislation. At this stage, it seems transposition is definitely still intended.

In the meantime, no changes were made regarding data retention. Some minor changes occurred in closely related areas (in general terms: see above, question 1).

On the scope of the obligation for operators to collaborate with policy and judiciary (mentioned in our answer to the previous question 23), we remind about the fact that the Highest Court has annulled the judgement of the Court of Appeal of Ghent (see

also answer to question 3), implying that providers of webmail services also have to collaborate according to art. 46bis CPC.

Finally, it can be mentioned that the reimbursement rates related to the obligation for operators to provide data to police and judiciary and the national intelligence and security have recently been decreased by 30% on average (for further details, see above, in our answer to question 2).

11. Please describe the following safeguards of the rule of law in detail:

a) catalogue of criminal offences falling under the "serious crime" definition: please provide a full list of criminal offences for the investigation, detection and prosecution of which retained data may be retrieved;

A catalogue of criminal offences falling under the "serious crime" definition is explicitly not foreseen by the draft act, because the government considered it unnecessary and inappropriate. The government is of the opinion that this requirement will have been fulfilled in a proportionate way by limiting the possibility to retrieve retained data only for the investigation, detection and prosecution of the two (out of three) most serious categories of criminal offences.

b) requirement of a court order prior to the data request: in essence, would such a court order be necessary, according to the (draft) data retention regime and other laws in effect (such as the criminal procedure code), before a request for access to retained data may be filed?

If this depends on the specific data requested (e.g. as far as traffic data are concerned, a court order would not be necessary, whereas access to location data may only be ordered by a court): please provide the criteria upon which the decision of whether or not a court order has to be sought is made.

As far as a court order is necessary: please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Are there any situations (e.g. "emergency cases") that are exempt from the requirement of a court order? If so: who will decide in these situations whether or not access to the data may be requested? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?

See question 17 previous report: "The draft data retention act and decree do not mention the need to obtain a specific court order before accessing the data retained, but in the case of law enforcement, the normal criminal procedure applies. According to these provisions, the more privacy-intruding mechanisms or measures can also be decided upon by an (independent) investigation judge. Subsidiarity and proportionality are the main principles in this respect, but the aggrieved party should not be heard or involved in the proceedings before the data is accessed."

In practice:

According to art. 46bis of the Criminal Procedure Code, the public prosecutor will be able to ask any operator to identify the subscriber or regular user of a specific telecommunications service, or to provide the identification data in relation to telecommunications services to which a person is subscribed or which he regularly uses. In very urgent cases, any officer of judicial police (i.e. senior police officers) can ask this services from the operator concerned.

According to art. 88bis of the CPC, an (independent) investigation judge will be able to ask operators access to their retained data in order to trace telecommunication, or to localise its origin or destination when he considers it necessary in order to reveal the truth. In case of catch in the act, the public prosecutor can also request this access, which later has to be confirmed by the investigation judge.

12. What considerations during the legislative procedure have led to the deviations between the Directive and the national law in terms of the *data categories to be retained*?

The considerations for the expansion of the categories of data to be retained are extensively discussed in the preparatory works of the draft act (see p. 26 - 31).

The justification of the additional identification data relates mainly to the fact that the government considers the expansion of identification data as necessary, reasonable and proportionate in order to reveal the real user of a communications service. In this respect, a number of additional data (e.g. invoicing address, payment data, technical data and additional subscription data) should be retained because they could possibly provide the only trail to the real user.

The justification of the additional traffic data also relates to the fact that the government considers the expansion of traffic data as necessary, reasonable and proportionate, but in this case because of its limited scope and the current approach. In this respect, operators will also have to retain the information about the location of the network connection point at the end of the connection, as well as the upload and download volume during an internet session.

13. As regards the purposes of retention/use of retained data:

a) In your answer to question 15, you mention that one of the three purposes of *use* of the retained data is "law enforcement (limited to serious crimes only) and the protection of national security, also through the access of intelligence services". Can you give the legal basis for the use of the data for the protection of national security (which is not mentioned in your answer to question 11 on the purposes of the *retention*)?

The access to retained data is not regulated by the draft data retention act, but for each purpose separately. The situation can be summarized as follows:

Criminal prosecution	**Art. 46bis and 88bis CPC**
Fight against malicious emergency calls	**Art. 107 ECA**
Fight against malicious calls through Ombudsdienst	**Art. 43 §3, 7° Act March 21st 1991**
Intelligence and security services	**Art. 18/7 18/8 and 18/17 of the act of November 30th 1998 on the intelligence and security services**

b) In your answers to questions 11 and 15 of the first questionnaire, you mention that data may be requested for the purpose of fighting "malicious calls". Is the term "malicious call" defined by law or jurisprudence? Is it a criminal offence in Belgium to make a "malicious call" (that is not covered by the data retention obligation for the purpose of fighting a "serious crime")? If so: Which other elements are required for this criminal offence to have been committed?

The context of the power attributed to the Ombudsdienst is not to the prosecution of any criminal offence, but the offering of a "service" to end-users. This service consists of revealing the identity and address of the malicious user to the requesting user. In its investigation, the Ombudsdienst can provide these data when they are available, and on the condition that the requesting user provides sufficient and precise proof and about the malicious calls. After having received this information, the user can turn to the police and judiciary authorities in order to file a complaint.

Causing nuisance or damage through the use of an electronic communications networks or service is a criminal offence which is punished with a fine from 275 to 1.650 euro and/or with imprisonment of 15 days to two year (see art. 145 §3bis ECA).

Based on the gravity of the penalties imposed, this criminal offence should be considered as a 'wanbedrijf' (offence of the second degree), for which the public prosecutor (art. 46bis CPC) and the investigation judge (art. 88bis CPC) can demand the collaboration of operators and/or access to their retained data.

14. The following questions refer to your answer to question 23 of the questionnaire and seek to clarify ambiguities which have arisen on the basis of Art. 3 of the draft law:

Artikel 3. Artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie wordt vervangen als volgt:	**Article 3.** L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques est remplacé par la disposition suivante :

"§ 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de operatoren die een openbare vaste telefoniedienst, een openbare mobiele telefoniedienst, een openbare internettoegangsdienst, een openbare emaildienst, of een openbare internettelefoniedienst aanbieden, de verkeers- en locatiegegevens en de gegevens voor identificatie van de eindgebruikers die door hen worden gegenereerd of verwerkt bij het aanbieden van hun respectievelijke elektronische-communicatienetwerken en –diensten, met het oog op:	« § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les opérateurs fournissant un service de téléphonie fixe accessible au public, un service de téléphonie mobile accessible au public, un service d'accès à l'Internet accessible au public, un service de courrier électronique accessible au public ou un service de téléphonie par Internet accessible au public, conservent les données de trafic, de localisation et les données d'identification d'utilisateurs finals qui sont générées ou traitées par eux lors de la fourniture respective de réseaux ou de services de communications électroniques, et ce en vue :

a) Please specify how your answer to question 23 of the first questionnaire is to be understood: Are providers of e-mail and internet telephony services obligated under the Belgian rules to retain data even where they do not provide, at the same time, an electronic communications service as defined in Art. 2 lit. c Directive 2002/21/EC? If so: Is it possible to say from the legislative records and/or the political debate if the legislator was aware of the fact that under the Directive only providers of publicly available electronic communications services and of public communications networks shall be obligated to retain data? According to the sources available to you, is the legislator of the opinion that it is not contrary to EU law to extend the scope of application in this way?

This issue is highly unclear. First, the ECA mainly had the objective to implement the EU Directives on electronic communications networks and services, but (being the general telecommunications act) also contains a number of provisions which fall outside the strict scope of the Directives (e.g. provisions on terminal equipment, provisions on 'other electronic communications services). In general terms, it seems reasonable to state that when the national act is using concepts such as "electronic communications network" or "electronic communications service", those concepts should generally be considered to be in line with the EU ones.

However, also the delimitation of the European concepts does not seems so straightforward as the question above seems to imply: what are providers of e-mail and internet telephony services which do not consist of an electronic communications service as defined in Art. 2 lit. c Directive 2002/21/EC? This lack of clarity also exists at Belgian national level and it is therefore highly unclear whether the ECA applies to them. As a consequence, it is also not clear whether the providers of such services should comply with the data retention provisions as put forward by the current article 126 of the ECA.

Related to this issue, is the legal discussion on the application of the obligation for operators to collaborate with police and judiciary and national intelligence and security services to the providers of such 'intermediate' communications services. The most relevant recent source of information in this respect, is the judgment of the Highest Court ('Hof van Cassatie') of January 18th 2011. In this judgement the Court annulled the judgement of the Court of Appeal of Ghent, which ruled that being a webmail provider, Yahoo! did not have to comply with the obligation to collaborate (see above, answer to question 3). Instead, the Highest Court is of the opinion that the interpretation to be given to the provisions of the Criminal Procedure Code should not reflect the interpretation (or delimitation) as it is given in the Electronic Communications Act.

Concluding, it therefore seems reasonable to state that at least the obligation to collaborate with police and judiciary (and in the future: to provide access to retained data for crime prosecution purposes) as mentioned in the Criminal Procedure Code also includes providers of e-mail and internet telephony services, even if they would not be considered as providers of electronic communications services under the ECA.

By explicitly including providers of "public email services" and/or "internet telephony services", the draft (new) article 126 seems to aim at mirroring this approach as regards the obligation to retain data.

It is not clear to what extent the legislator considers imposing retention obligations on providers of e-mail and internet telephony services (which would not also qualify as electronic communications service) as not in line with the Data Retention Directive. Based on the preparatory works (and the explicatory memorandum accompanying the act) it seems the legislator is of the opinion that these services should always be considered as public electronic communications services, thereby also falling within the scope of the Electronic Communications and Data Retention Directives.

b) Are operators of public communications *networks* specifically exempt by law from the obligation to retain data, e.g. through specific rules that seek to prevent the same data from being retained more than once (which would be the case where the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.

The current version of the texts only refers to 'operators' (i.e. providers) of a number of public electronic communications *services* and does not include any reference to operators of networks. The situation in which the provider of the service is different from the operator of the network, and where data need to be retained by the latter, does not seem to be covered.

c) **Does the law provide a more specific definition of the term "private network", as mentioned in your answer to question 23 of the first questionnaire?**

The term 'private network' is not defined in the ECA, but the issue is not relevant for the application of data retention provisions.

15. **Please describe the latest developments with regard to the reimbursement of costs. Which costs are reimbursed according to the current state of the discussion? As far as available: In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process used in the context of service provision, billing and related business activities?**

In relation to data retention, there are no new developments. Our answer on question 28 of the previous report remains valid. As mentioned above, the reimbursement rates for the collaboration of operators with police and judiciary authorities and national intelligence and security services of have been decreased by 30% on average (see above, question 2). The actual reimbursement rates can be found in the annex to the Royal decree February 8th 2011.

16. **Please give more details about where and how the data is stored (see your answers to questions 38 and 39 of the first questionnaire): is it possible today to provide further information about how storage of the data to be retained is effected in practice? Does Belgian law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC?**

Regarding storage of retained data, no additional details have been made public. The draft act on data retention does not contain specific procedures or provisions on the transfer of personal data to third countries. The act however stipulates that the provisions of the general data protection act (articles 22-23 of the Act of December 8th 1992) remain applicable. Further, specific rules about the collaboration with authorities in third countries also exist in the area of criminal law.

17. **Which EU legislative acts and international treaties on cross-border co-operation (i.e. rules specifically designed for data retention as well as general rules applicable to data retention) are applied in Belgium? What do the rules applicable to data retention provide?**

Besides the general EU legislative and regulatory framework, the most important international sources of legislation are:

- regarding cybercrime
  - Convention of cybercrime, Council of Europe, Budapest 23 Nov. 2001

- regarding protection of privacy:
  - European Convention for the protection of Human Rights and Fundamental freedoms of 1950, ECHR Convention
  - Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data of 28 January1981, Convention 108
  - OECD Guidelines governing the protection of Privacy and transborder data flows of personal data of 20 September 1980

Since most of these texts have been incorporated or implemented in European and/or Belgian national law, their additional impact on the data retention aspects remains quite limited.

18. Please provide more details on the *scope of competence* (data retention obligations, data protection rules) of the supervisory authorities referred to in your answer to question 35 of the first questionnaire.

Which public bodies are responsible for supervising that the *bodies entitled to obtain access to the data retained* (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

First, it should be recalled that abuse of the retained (personal) data can be punished under a number of general criminal law provisions (e.g. external or internal hacking), as well as under the criminal provisions in the general data protection act. Further, the draft act also creates a new specific offence since breaching the provisions of the act will be punished as a criminal offence, potentially leading up to a fine of 275€ or 3 year of imprisonment. The regular (criminal) courts by consequence have the most important role in guaranteeing the compliancy with the provisions of the act.

Second, the data protection authority supervises the correct application of the data protection act. In case retained data would not be processed in compliancy with the general data protection provisions, a complaint can be filed to the data protection authority which will examine the case and try to mediate between the parties. If no compromise can be found, the data protection authority can publish an official report and provide it viewpoint on the issue. Non-compliancy with the provisions of the data protection act constitutes a criminal offence.

According to the articles 14, 3° and 21 of the Act of January 17th 2003, the Belgian Telecommunications regulatory authority (BIPT) has the general power of supervising the correct application of the ECA. In case of non-compliancy, the BIPT can impose administrative fines up to 12,5 million euro.

Ultimately, the "coordination cell justice" of each operator is responsible for the fact that all processing of data happens in compliance with the legal provisions. The department and minister of Justice have a general supervisory role over them, since they can refuse a person to function within the coordination cell justice (art. 2 Royal decree of January 9th 2003).

19. **Please describe the procedure and the sanctions available to the privacy commission when punishing violations of data protection rules, and to the respective supervisory authority for any other misdemeanours in the context of data retention.**

    See previous question.

20. **Apart from the criminal offence explained in your answer to question 30 of the first questionnaire: are there any other criminal or administrative sanctions foreseen in case that data retention rules are not complied with?**

    See previous question: 1° general criminal law; 2° data protection criminal offences; 3° administrative fines imposed by the telecommunications regulator.