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

United Kingdom

Andrew Charlesworth

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?

Directive 2006/24/EC was transposed into UK law in two key stages. The initial stage of transposition was via the *Data Retention (EC Directive) Regulations 2007* (SI 2007 No. 2199) which covered fixed network telephony and mobile telephony communications providers. The Data Retention Directive permitted Member States to postpone application of the Directive to the retention of communications data

relating to internet access, internet telephony and internet e-mail,[1] and the UK delayed implementation in those areas until the *Data Retention (EC Directive) Regulations 2009* (SI 2009 No. 859), which then replaced and repealed the 2007 Regulations.[2] Discussion in this document will refer to the 2009 Regulations.

It had been intended that the Directive would be transposed via a proposed Communications Data Bill, which was described in the UK Government's draft legislative programme for 2008/09, *Preparing Britain for the future*,[3] as follows:

> "…The purpose of the Bill is to: allow communications data capabilities for the prevention and detection of crime and protection of national security to keep up with changing technology through providing for the collection and retention of such data, including data not required for the business purposes of communications service between privacy and protecting the public.
>
> The main elements of the Bill are:
>
> - Modify the procedures for acquiring communications data and allow this data to be retained;
> - Transpose EU Directive 2006/24/EC on the retention of communications data into UK law."

However, public controversy about the likely contents of the Communications Data Bill resulted in a delay in its publication, and it was decided instead to complete the transposition of the Directive via secondary legislation in order to meet the deadline of March 2009 laid down in the Directive.

- ***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 delay in implementing the retention of communications data relating to internet access, internet telephony and internet e-mail until March 2009 was expressly permitted by the Directive. The UK government's rationale for choosing to delay implementation in these areas was that "This postponement allows extra time to consider the more complex implementation issues associated with this type of

---

1 Art.15(3) DRD.

2 See Claire Walker, 'Data retention in the UK: Pragmatic and proportionate, or a step too far?' (2009) 25(4) *Computer Law & Security Review,* 325.

3 *Preparing Britain for the future*. TSO, May 2008, 52-53.
http://www.official-documents.gov.uk/document/cm73/7372/7372.pdf

data."[4] These implementation issues were discussed in the UK government's consultation document of August 2008.[5] They centred less upon wider policy issues and concerns, such as privacy, and more upon practical matters, such as:

- the clarity of the application of implementing legislation to the activities of communication providers;
- the clarity of definition of the types of data to be retained;

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?

Transposition of Directive 2006/24/EC itself is complete. However, the processes through which retained data will be collected, stored and accessed are the subject of continuing discussion.

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.

There are no further draft legal acts in train concerning implementation of Directive 2006/24/EC, nor, at the time of writing, are there any outstanding legal actions or court decisions with regard to the legality of the *Data Retention (EC Directive) Regulations 2009*.

- ***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.

UK Statutory Instruments are numbered, catalogued, and made available for sale in print form, and without charge via the internet.

Data Retention (EC Directive) Regulations 2007 (now repealed)
http://www.legislation.gov.uk/uksi/2007/2199/made (HTML)
http://www.legislation.gov.uk/uksi/2007/2199/made/data.pdf (PDF)

Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2007
http://www.legislation.gov.uk/uksi/2007/2199/pdfs/uksiem_20072199_en.pdf (PDF)

Data Retention (EC Directive) Regulations 2009 (in force)
http://www.legislation.gov.uk/uksi/2009/859/made (HTML)

---

4 *Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2007*, para. 4.2.

5 Home Office, *A consultation paper: Transposition of Directive 2006/24/EC*, August 2008 http://www.statewatch.org/news/2008/aug/uk-ho-consult-mand-ret-internet.pdf

http://www.legislation.gov.uk/uksi/2009/859/made/data.pdf (PDF)

Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009
http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksiem_20090859_en.pdf (PDF)

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

The *Data Retention (EC Directive) Regulations 2007* were made on 26th July 2007, and came into force on 1st October 2007. They were repealed on 6th April 2009 when the *Data Retention (EC Directive) Regulations 2009*, which were made on 2nd April 2009, came into force. The *Data Retention (EC Directive) Regulations 2009* remain in force. Neither set of Regulations contained significant transitional periods.

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.

The Directive could have been implemented in the UK via either primary or secondary legislation – there are no set rules and the choice is at the discretion of the responsible Minister. Normally, primary legislation would be used where no pre-existing powers exist to give effect to the particular Community legislation, and secondary legislation used where national legislation already provides specific powers to enact legislation on the subject matter in question.[6] In some cases, transposition measures may be incorporated into omnibus primary legislation veering a range of related subject matter. As noted in Q1, the transposition of Directive 2006/24/EC was to have been via the proposed Communications Data Bill – when this was dropped by the government, a rapid solution was required to meet the deadline.

The rationale for choosing secondary legislation thus appears largely to have been the need to meet the deadline for implementation in the Directive.

---

6 Bates, T. United Kingdom Implementation of EU Directives, (1996) 17(1) *Statute Law Review*: 27-49.

> While consideration had been given to completing the transposition of the data retention directive using a Communications Data Bill, the decision to use secondary legislation is consistent with the approach which led to the Data Retention (EC Directive) Regulations SI 2007/2199…[7]

The *Data Retention (EC Directive) Regulations 2009* are Statutory Instruments (SIs). SIs are the commonest form of UK subordinate legislation (also known as secondary or delegated legislation). They are made by or under powers conferred by or under statute on Her Majesty in Council or on a Minister, and provide the detailed regulations which implement Acts of Parliament.

The *Data Retention (EC Directive) Regulations 2009* were made by the Secretary of State[8] under powers conferred by s.2(2) of the European Communities Act 1972.[9] They were subject to the 'affirmative resolution procedure' for SIs. This procedure requires that the SI in question must be approved by both the House of Commons and the House of Lords.[10] The affirmative resolution procedure is used primarily for potentially controversial legislation, and is used for about 10% of SIs subject to parliamentary control. Neither House can amend or adapt the SI during the procedure, but if either House rejects it, it cannot pass into law.

---

7 Grahame Danby, *Draft Communications Data Bill*, Library of the House of Commons SN/HA/48846 January 2009 at 1.

8 Under the UK Interpretation Act 1978, "Secretary of State" means one of Her Majesty's Principal Secretaries of State. UK legislation generally does not refer to a specific Secretary of State. The draft Regulations were introduced to Parliament by Vernon Coaker, then Minister of State at the Home Office with responsibility for Policing. The "Secretary of State" in question will thus be the Home Secretary.

9 *European Communities Act 1972*: s.2(2) Subject to Schedule 2 to this Act, at any time after its passing Her Majesty may by Order in Council, and any designated Minister or department may by order, rules, regulations or scheme, make provision—

> (a) for the purpose of implementing any EU obligation of the United Kingdom, or enabling any such obligation to be implemented, or of enabling any rights enjoyed or to be enjoyed by the United Kingdom under or by virtue of the Treaties to be exercised; or
>
> (b) for the purpose of dealing with matters arising out of or related to any such obligation or rights or the coming into force, or the operation from time to time, of subsection (1) above;

and in the exercise of any statutory power or duty, including any power to give directions or to legislate by means of orders, rules, regulations or other subordinate instrument, the person entrusted with the power or duty may have regard to the objects of the EU and to any such obligation or rights as aforesaid.

In this subsection "designated Minister or department" means such Minister of the Crown or government department as may from time to time be designated by Order in Council in relation to any matter or for any purpose, but subject to such restrictions or conditions (if any) as may be specified by the Order in Council.

10 See House of Commons Information Office, *Statutory Instruments* Factsheet L7 Legislative Series (FS No.L7 Ed 3.9) Revised May 2008,

http://www.parliament.uk/documents/commons-information-office/l07.pdf

The draft *Data Retention (EC Directive) Regulations 2009* were published on 18 February 2009.[11] They were debated in the House of Commons Delegated Legislation Committee on 16 March 2009.[12] The Motion to approve the Regulations took place without debate in the House of Commons on 17 March 2009 with 241 votes for and 93 votes against.[13] The Motion to approve the Regulations and resulting debate took place in the House of Lords on 24 March 2009 with 93 votes for and 89 votes against.[14]

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 definitions in Art 2, para 2 of Directive 2006/24/EC and the *Data Retention (EC Directive) Regulations 2009* are juxtaposed below:

> Directive 2006/24/EC, Art 2(2)(a) - 'data' means traffic data and location data and the related data necessary to identify the subscriber or user.
>
> Regulations Reg. 2(b) - "communications data" means traffic data and location data and the related data necessary to identify the subscriber or user.

Definition is identical but UK legislation specifies communications data rather than just data, presumably to clarify that content data is not included.

> Directive 2006/24/EC, Art 2(2)(b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;
>
> Regulations – no definition.

The term 'user' is not defined in the Regulations.

---

11 The Stationary Office, Daily List no. 034, for Titles published on Wednesday 18 February 2009

http://www.tso.co.uk/daily_list/issues/2009/dl034.htm

12 HC Delegated Legislation Committee, Draft Data Retention (EC Directive) Regulations 2009, 16 March 2009.

http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm

13 HC Deb, 17 March 2009, c877.

http://www.parliament.the-stationery-office.com/pa/cm200809/cmhansrd/cm090317/debtext/90317-0019.htm

14 HL Deb, 24 March 2009, c620-639.

http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/90324-0011.htm#09032466000001

> Directive 2006/24/EC, Art 2(2)(c) - 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services).
>
> Regulations Reg. 2(f) – 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services).

The definition in the Regulations is identical to the English language version of the Directive

> Directive 2006/24/EC, Art 2(2)(d) - 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service
>
> Regulations Reg. 2(h) - 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an internet access service or internet communications service.

The definition in the Regulations is identical to the definition in the English language version of the Directive

> Directive 2006/24/EC, Art 2(2)(e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated.
>
> Regulations Reg. 2 (a) "cell ID" means the identity or location of the cell from which a mobile telephony call started or in which it finished;

The definition in the Regulations adds 'or location' to the definition in the English language version of the Directive.

> Directive 2006/24/EC, Art 2(2)(f) - 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.
>
> Regulations Reg. 4(3) – … 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

The definition in the Regulations is identical to the definition in the English language version of the Directive.

The *Data Retention (EC Directive) Regulations 2009* contains the following additional definitions:

> Reg. 2(c) - "the Data Retention Directive" means Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

This simply refers back to Directive 2006/24/EC as the legislation that the Regulations are implementing.

> Reg. 2(d) - “location data” means data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—
>
> (i) the latitude, longitude or altitude of the terminal equipment,
>
> (ii) the direction of travel of the user, or
>
> (iii) the time the location information was recorded.
>
> Directive 2002/58/EC, Art. 2(c) - "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

The definition in the Regulations is clearly drawn from, but more precise than, that contained in Directive 2002/58/EC. This is likely an artefact of Parliamentary drafting.[15]

> Reg. 2(e) - “public communications provider” means—
>
> (i) a provider of a public electronic communications network, or
>
> (ii) a provider of a public electronic communications service;
>
> and “public electronic communications network” and “public electronic communications service” have the meaning given in section 151 of the Communications Act 2003
>
> > UK Communications Act 2003 s.151 - ‘public electronic communications network’ an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.
> >
> > UK Communications Act 2003 s.151 - ‘public electronic communications service’ as any electronic communications service that is provided so as to be available for use by members of the public.
>
> Directive 2002/21/EC, Art 2 (d) - "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

The definition in the Regulations is clearly inherited from the definition contained in Directive 2002/21/EC

> Reg. 2 (g) - “traffic data” means data processed for the purpose of the conveyance of a communication on an electronic communications

---

15 EU legislation, particularly in Directives, tends to be drawn up in more general terms than UK legislation.

network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication;

Directive 2002/58/EC, Art. 2 (b) - "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

The definition in the Regulations is clearly drawn from, but more precise than, that contained in Directive 2002/58/EC. This is likely an artefact of Parliamentary drafting.

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?

According to Reg. 4 (1) DRR, the data specified in Parts 1-3 of the Schedule to the Regulations must be retained.

(a) Part 1 refers to fixed network telephony;

(b) Part 2 refers to mobile telephony;

(c) Part 3 refers to internet access, internet e-mail or internet telephony.

See Tables 1-3 below for a comparison between the provisions of the Directive and those of the Regulations. The table suggests a close correspondence between the Directive and Regulations.

In Reg. 4(2) DRR it is stated that unsuccessful call attempts that:

(a) in the case of telephony data, are stored in the United Kingdom, or

(b) in the case of internet data, are logged in the United Kingdom

must be retained. This obligation does not extend to unconnected calls.

Table 1 – Fixed network telephony

Type of Data	Directive 2006/24/EC	Data Retention (EC Directive) Regulations 2009
Fixed network telephony	Art.5(1)(a) - Data necessary to trace and identify the source of a communication: • the calling telephone number; • the name and address of the subscriber or registered user	Part 1(1) - Data necessary to trace and identify the source of a communication • the calling telephone number. • the name and address of the subscriber or registered user of any such telephone.
	Art.5(1)(b) - Data necessary to identify the destination of a communication • the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed; • the name(s) and address(es) of the subscriber(s) or registered user(s).	Part 1(2) - Data necessary to identify the destination of a communication • the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred. • the name and address of the subscriber or registered user of any such telephone.
	Art.5(1)(c) - Data necessary to identify the date, time and duration of a communication • the date and time of the start and end of the communication	Part 1(3) - Data necessary to identify the date, time and duration of a communication • the date and time of the start and end of the call.
	Art.5(1)(d) - Data necessary to identify the type of communication • the telephone service used	Part 1(4) - Data necessary to identify the type of communication • the telephone service used.
	Art.5(1)(e) - Data necessary to identify users' communication equipment or what purports to be their equipment • the calling and called telephone numbers	Omitted, probably because it duplicates the information to be retained under Part 1(1) & (2)

Table 2 – Mobile telephony

Type of Data	Directive 2006/24/EC	Data Retention (EC Directive) Regulations 2009
Mobile telephony	Art.5(1)(a) - Data necessary to trace and identify the source of a communication: • the calling telephone number; • the name and address of the subscriber or registered user	Part 2(5) - Data necessary to trace and identify the source of a communication • the calling telephone number. • the name and address of the subscriber or registered user of any such telephone.
	Art.5(1)(b) - Data necessary to identify the destination of a communication • the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed; • the name(s) and address(es) of the subscriber(s) or registered user(s).	Part 2(6) - Data necessary to identify the destination of a communication • the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred. • the name and address of the subscriber or registered user of any such telephone.
	Art.5(1)(c) - Data necessary to identify the date, time and duration of a communication • the date and time of the start and end of the communication	Part 2(7) - Data necessary to identify the date, time and duration of a communication • the date and time of the start and end of the call.
	Art.5(1)(d) - Data necessary to identify the type of communication • the telephone service used	Part 2(8) - Data necessary to identify the type of communication • the telephone service used.
	Art.5(1)(e) - Data necessary to identify users' communication equipment or what purports to be their equipment • the calling and called telephone numbers; • the International Mobile Subscriber Identity (IMSI) of the calling party; • the International Mobile Equipment Identity (IMEI) of the calling party; • the IMSI of the called party; • the IMEI of the called party; • in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;	Part 2(9) - Data necessary to identify users' communication equipment (or what purports to be their equipment) • the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made. • the IMSI and the IMEI of the telephone dialled. • in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated Calling and called telephone numbers omitted, probably because this duplicates the information to be retained under Part 2(5) & (6)
	Art.5(1)(f) - Data necessary to identify the location of mobile communication equipment • the location label (Cell ID) at the start of the communication; • data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.	Part 2(10) - Data necessary to identify the location of mobile communication equipment • the cell ID at the start of the communication. • data identifying the geographic location of cells by reference to their cell ID.

Table 3 – Internet access, Internet E-mail and Internet telephony

Type of Data	Directive 2006/24/EC	Data Retention (EC Directive) Regulations 2009
Internet access, Internet E-mail and Internet telephony	Art 5(1)(a) - Data necessary to trace and identify the source of a communication: • the user ID(s) allocated; • the user ID and telephone number allocated to any communication entering the public telephone network; • the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication	Part 3(11) - Data necessary to trace and identify the source of a communication • the user ID allocated. • the user ID and telephone number allocated to the communication entering the public telephone network. • the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.
	Art 5(1)(b) - Data necessary to identify the destination of a communication • the user ID or telephone number of the intended recipient(s) of an Internet telephony call; • the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;	Part 3(12) - Data necessary to identify the destination of a communication • in the case of internet telephony, the user ID or telephone number of the intended recipient of the call. • in the case of internet e-mail or internet telephony, the name and address of the subscriber or registered user and the user ID of the intended recipient of the communication.
	Art 5(1)(c) - Data necessary to identify the date, time and duration of a communication • the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user; • the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone	Part 3(13) - Data necessary to identify the date, time and duration of a communication • in the case of internet access: o the date and time of the log-in to and log-off from the internet access service, based on a specified time zone, o the IP address, whether dynamic or static, allocated by the internet access service provider to the communication, and o the user ID of the subscriber or registered user of the internet access service. • in the case of internet e-mail or internet telephony: o the date and time of the log-in to and log-off from the internet e-mail or internet telephony service, based on a specified time zone.
	Art 5(1)(d) - Data necessary to identify the type of communication • the Internet service used	Part 3(14) - Data necessary to identify the type of communication • in the case of internet e-mail or internet telephony, the internet service used.
	Art 5(1)(e) - Data necessary to identify users' communication equipment or what purports to be their equipment • the calling telephone number for dial-up access; • the digital subscriber line (DSL) or other end point of the originator of the communication.	Part 3(15) - Data necessary to identify users' communication equipment (or what purports to be their equipment) • in the case of dial-up access, the calling telephone number. • in any other case, the digital subscriber line (DSL) or other end point of the originator of the communication.

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 Regulations make no provision 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.

The Privacy and Electronic Communications (EC Directive) Regulations 2003[16] place restrictions upon the collection of certain traffic data (Regs.7-8) and location data (Reg.14). The Regulations do permit traffic data relating to subscribers or users to be processed and stored by a public communications provider for:

- purposes connected with the payment of charges by a subscriber, or in respect of interconnection payments, until the end of the period during which legal proceedings may be brought in respect of payments due or alleged to be due or, where such proceedings are brought within that period, the time when those proceedings are finally determined.[17]

- the purpose of marketing electronic communications services, or for the provision of value added services to that subscriber or user, where the subscriber or user to whom the traffic data relate has given his consent (and not subsequently withdrawn it), and the processing and storage are undertaken only for the duration necessary for those purposes.[18]

In both cases, the subscriber or user to whom the data relate must have been provided with information regarding the types of traffic data which are to be processed and the duration of such processing, and in the second case, have been provided with that information before their consent has been obtained.[19]

Processing is restricted to what is required for the purposes of one or more of the following activities:

- the management of billing or traffic;
- customer enquiries;
- the prevention or detection of fraud;
- the marketing of electronic communications services;
- the provision of a value added service.

---

16 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003 No. 2426) http://www.legislation.gov.uk/uksi/2003/2426/contents/made

17 Reg. 7(2), 7(5), PECR 2003.

18 Reg. 7(3), PECR 2003.

19 Reg. 8, PECR 2003.

and may be carried out only by the public communications provider or by a person acting under their authority.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 do not prevent the provision of traffic data to a person who is a competent authority for the purposes of any provision relating to the settling of disputes (by way of legal proceedings or otherwise) which is contained in, or made by virtue of, any enactment.[20]

The Privacy and Electronic Communications (EC Directive) Regulations 2003 permit the processing of (but are silent on storage of) location data where:

- the user or subscriber cannot be identified from such data; or
- where the processing is necessary for the provision of a value added service, with the consent of that user or subscriber (which may be withdrawn absolutely or with regard to specific communications).[21]

Where user or subscriber consent is sought, the public communications provider in question must provide the following information about

- the types of location data that will be processed;
- the purposes and duration of the processing of those data; and
- whether the data will be transmitted to a third party for the purpose of providing the value added service.[22]

Processing of location data may be carried out only by the public communications provider, the third party providing the value added service, or by a person acting under either of their authority. Where processing is carried out for the purposes of the provision of a value added service, it must be restricted to what is necessary for those purposes.[23]

The Regulation of Investigatory Powers Act 2000[24] provides for lawful interception of communications content in the course of its transmission via a public telecommunication system within the UK with and without a warrant from the Secretary of State.[25] An interception made intentionally and without lawful authority will be an offence.[26] Data collected in the course of a lawful interception under warrant may only be held until there are no longer any grounds for retaining it as

---

20 Reg. 8(4), PECR 2003.

21 Reg. 14, PECR 2003.

22 Reg. 14(3), PECR 2003.

23 Reg. 14(5), PECR 2003.

24 The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2005 (SI 2005 No. 1083)

http://www.legislation.gov.uk/uksi/2005/1083/made (HTML)

25 s.3 & s.5 RIPA 2000.

26 s.1, RIPA 2000.

necessary for any of the authorised purposes under the Act.[27] The role of the Regulation of Investigatory Powers Act 2000 in the acquisition and disclosure of communications data, as opposed to communications content, is discussed below.

Except insofar as provided for by the Data Retention (EC Directive) Regulations 2009, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Regulation of Investigatory Powers Act 2000, retention of electronic communications data (customer records, traffic data and/or the content of communications) where an individual can be identified by or linked to that data, unless one of the conditions for processing in Schedule 2 DPA 1998 is met (i.e. where a user or subscriber has given their consent), would appear to be barred by the requirements of the Data Protection Act 1998.

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

The Regulations are silent on the purposes for which data retention is mandated. Access to data retained is governed by the Regulation of Investigatory Powers Act 2000, Chapter II - Acquisition and disclosure of communications data, s21-25. (see below)

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)?

On the assumptions that this question:

a) refers to communication data and not content data, and that

b) the term 'sensitive data' is not being used in the sense used in Directive 95/46/EC,

then there are no specific rules in national law prohibiting the retention and/or transmission of sensitive data. Even if the data collected did in some way fall within the scope of Directive 95/46/EC, then with regard to the UK implementing legislation, the Data Protection Act 1998, it seems clear that retention and/or transmission of such data would still be permitted under the exemptions in Part IV DPA 1998.

---

[27] s.15(3), RIPA 2000. e.g. in the interests of national security; for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the United Kingdom; for giving effect to the provisions of any international mutual assistance agreement; for facilitating the functions of the Secretary of State, the Interception of Communications Commissioner or the Tribunal; to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution.

The UK House of Lords (now the UK Supreme Court) ruled in 2009 in *In re McE (Appellant) (Northern Ireland)* that the Regulation of Investigatory Powers Act (RIPA) can override legal professional privilege with regard to covert electronic surveillance (Part II RIPA).[28] While acquisition and disclosure of communications data is in Part I of RIPA 2000 and was not therefore the subject of the case, the discussion in that case regarding legal professional privilege is instructive, notably at para. 81:

> "It is to be noted that [the] authorities dealing with [legal professional] privilege were all concerned with the use of evidence consisting of <u>what was said between legal advisers and clients</u>. The rule preventing that remains absolute…" (my emphasis).

Thus, it appears that communications data itself, inasmuch as it specifically does not constitute 'what was said between legal advisers and clients' would therefore not attract legal professional privilege.

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.

Reg.5 states that "The data specified in the Schedule to these Regulations must be retained by the public communications provider for a period of 12 months from the date of the communication in question." No distinction is made between data categories.

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)?

Reg.7 DRR states that:

> Access to retained data
>
> 7. Access to data retained in accordance with these Regulations may be obtained only—
>
> (a) in specific cases, and
>
> (b) in circumstances in which disclosure of the data is permitted or required by law.

It has been pointed out by many commentators that this is not necessarily a very restrictive definition, as Parliament (and possibly the courts, through disclosure

---

[28] In re McE (Appellant) (Northern Ireland), In re C (AP) and another (Appellants) (Northern Ireland), In re M (Appellant) (Northern Ireland) [2009] UKHL 15.

orders such as Norwich Pharmacal Orders[29]) may permit or require that further public and private bodies be granted access to retained data.

Since its coming into force, access to retained data has been governed by the Regulation of Investigatory Powers Act 2000, Chapter 2 - Acquisition and disclosure of communications data s.21-25. [30] The provisions thus applied to data retained under the Code of Practice for Voluntary Retention of Communications (2004-2007), Data Retention (EC Directive) Regulations 2007 (2007-2009) and to the current Data Retention (EC Directive) Regulations 2009 (2009-).

S.25(1) RIPA defines "relevant public authority" for the purpose of acquisition and disclosure of communications data. It also confers powers on the Secretary of State to designate additional public authorities for the purpose of that definition.

> 25(1) RIPA: In this Chapter—
>
> "relevant public authority" means ... any of the following—
>
> (a) a police force;
>
> (b) the Serious Organised Crime Agency;[31]
>
> (ba) the Scottish Crime and Drug Enforcement Agency;[32]
>
> (d) Her Majesty's Revenue and Customs[33]
>
> (f) any of the intelligence services;
>
> (g) any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State.

After the passage of the RIPA 2000, the UK government expanded/amended the number of bodies who could have access to communications data via the following statutory instruments:

The Regulation of Investigatory Powers (Communications Data) Order 2003

---

29 A Norwich Pharmacal order is an exception to the general rule that only people who are actually named as parties to existing litigation are obliged to disclose documents and other materials relevant to the claims.

30 See House of Lords, Written answers and statements, HL Deb, 20 April 2009, c322-323.

http://www.publications.parliament.uk/pa/ld200809/ldhansrd/text/90420w0004.htm#09042043002193

31 s.25(1) RIPA 2000: para. (c) in the definition of "relevant public authority" substituted (1.4.2006) for paras. (c)(d) by Serious Organised Crime and Police Act 2005 (c. 15), ss. 59, 178, Sch. 4 para. 135(2); S.I. 2006/378, art. 4(1), Sch. para. 10 (subject to art. 4(2)-(7)).

32 s.25(1) RIPA 2000: para (ba) in the definition of "relevant public authority" inserted (1.4.2007) by The Police, Public Order and Criminal Justice (Scotland) Act 2006 (Consequential Provisions and Modifications) Order 2007 (S.I. 2007/1098), arts. 1(3), 6, Sch. para. 4(5).

33 s.25(1) RIPA 2000: paras. (d), (e), in the definition of "relevant public authority" substituted (15.2.2008) for para. (d) by Serious Crime Act 2007 (c. 27), ss. 88, 94 {Sch. 12 para. 8}; S.I. 2008/219, art. 2(b).

http://www.legislation.gov.uk/uksi/2003/3172/made (HTML)

The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2005 (SI 2005 No. 1083)
http://www.legislation.gov.uk/uksi/2005/1083/made (HTML)

The Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 (SI 2006 No. 1878)
http://www.legislation.gov.uk/uksi/2006/1878/made (HTML)

These statutory instruments were revoked in 2010 by a consolidating Order:

The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010 No. 480)
http://www.legislation.gov.uk/uksi/2010/480/made (HTML)

Under s.25(2) RIPA, the persons designated for the purposes of Chapter 2 are individuals holding such offices, ranks or positions with relevant public authorities as are prescribed by order of the Secretary of State. Under section 25(3)(a), restrictions can be placed by such an order on the authorisations under section 22(3) and the notices under section 22(4) that may be granted or given by an individual holding an office, rank or position with a specified public authority. See further Table 4. Under section 25(3)(b), the purposes for which such authorisations may be granted or notices may be given may be restricted by order. See further Table 4.

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)?

S.22 RIPA 2000 permits a person designated for the purposes of Chapter 2 (acquisition and disclosure of communications data) of Part 1 of RIPA:

- where they believe that it is necessary to obtain communications data for specified purposes falling within that section or within The Regulation of Investigatory Powers (Communications Data) Order 2010 – s.22 (1) & s.22(2);
    - to grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as the designated person to engage in any conduct to which Chapter 2 applies - s.22(3);
    - to issue a notice to a postal or telecommunications operator who is, or may be in possession of, or able to obtain, any communications data required for authorised purposes under s.22(2), requiring the operator to obtain the data (if not in possession of it) and to disclose all of the data in his possession or subsequently obtained - s.22(4

The specified purposes are:

> 22(2) RIPA: It is necessary on grounds falling within this subsection to obtain communications data if it is necessary—
>
> (a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
>
> (c) in the interests of the economic well-being of the United Kingdom;
>
> (d) in the interests of public safety;
>
> (e) for the purpose of protecting public health;
>
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
>
> (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
>
> (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010 No. 480) Art.2 adds additional grounds to those in s.22(2) RIPA:

> Art. 2. The following additional purposes are specified for the purposes of section 22(2) of the Act (to the extent that they do not fall within paragraphs (a) to (g) of that provision)—
>
> (a) to assist investigations into alleged miscarriages of justice;
>
> (b) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
>
> (i) to assist in identifying P, or
>
> (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

See further Table 4.

Table 4 – Access to retained data under RIPA 2000 and Regulation of Investigatory Powers (Communications Data) Order 2010.

Section 1. Individuals in body authorised under s.25 (1) (a)-(f) RIPA 2000: Public authorities that may acquire all types of communications data within s.21(4) of RIPA	**Prescribed offices (generally all communications data)**	**Additional prescribed offices (communications data falling within s.21(4)(c) RIPA)**	**Reason under s.22(2) RIPA or Art.2 2010 Order**
A police force maintained under s.2 of the Police Act 1996	Superintendent	Inspector	(a), (b), (c), (d), (e),(g) Art.2(b)
The metropolitan police force	Superintendent	Inspector	(a), (b), (c), (d), (e),(g) Art.2(b)
The City of London police force	Superintendent	Inspector	(a), (b), (c), (d), (e),(g) Art.2(b)
A police force maintained under or by virtue of s. 1 of the Police (Scotland) Act 1967	Superintendent	Inspector	(a), (b), (c), (d), (e),(g) Art.2(b)
The Police Service of Northern Ireland	Superintendent	Inspector	(a), (b), (c), (d), (e),(g) Art.2(b)
The Ministry of Defence Police	Superintendent	Inspector	(a), (b), (c), (g)
The Royal Navy Police	Commander	Lieutenant Commander	(a), (b), (c), (g)
The Royal Military Police	Lieutenant Colonel	Major	(a), (b), (c), (g)
The Royal Air Force Police	Wing Commander	Squadron Leader	(a), (b), (c), (g)
The British Transport Police	Superintendent	Inspector	(a), (b), (c), (d), (e), (g) Art. 2(b)
The Commissioners for Her Majesty's Revenue and Customs	Senior Officer	Higher Officer	(b), (f)
The Serious Organised Crime Agency	Senior Manager (Grade 2)	Principal Officer (Grade 3)	(b), (g) Art.2(b)
The Scottish Crime and Drug Enforcement Agency	Superintendent or Grade PO7	Inspector	(b), (d), (g)
The Security Service	General Duties 3 or any other officer at level 3	General Duties 4	(a), (b), (c)
The Secret Intelligence Service	Grade 6 or equivalent	—	(a), (b), (c)
The Government Communications Headquarters	GC8	—	(a), (b), (c)

Individuals in additional bodies authorised under s.25(1)(g) RIPA by Regulation of Investigatory Powers (Communications Data) Order 2010. Public authorities that may acquire all types of communications data within s.21(4) of RIPA.	**Prescribed offices (All authorisations/notices)**	**Additional prescribed offices (Authorisations/notices relating solely to communications data falling within s.21(4)(c) RIPA)**	**Reason under s.22(2) RIPA or Art.2 2010 Order**
The Department for Transport	Coastal Safety Manager (Grade 7) Maritime & Coastguard Agency	Rescue Coordination Centre Manager, Maritime & Coastguard Agency	(g)
	Inspector, Air Accident Investigation Branch, the Marine Accident Investigation Branch or the Rail Accident Investigation Branch	—	(d)
The Home Office	Immigration Inspector or Senior Officer, or Immigration Inspector or Senior Executive Officer with responsibility for anti-corruption, UK Border Agency	—	(b)
	Head of Security and Intelligence (Detention Services), UK Border Agency	—	(b), (d) Art.2(b)
The Ministry of Justice	Manager of the National Intelligence Unit of the National Offender Management Service	Manager in the National Intelligence Unit of the National Offender Management Service	(b), (d) Art. 2(b)
The Northern Ireland Office	Governor 4 in the N. Ireland Prison Service	—	(b), (d) Art.2(b)
The Civil Nuclear Constabulary	Superintendent	Inspector	(a), (b)
The force comprising the special constables appointed under s. 79 of the Harbours, Docks and Piers Clauses Act 1847 on the nomination of the Dover Harbour Board	Superintendent	Inspector	(b), (d), (e) Art.2(b)
The force comprising the constables appointed under art. 3 of the Mersey Docks and Harbour (Police) Order 1975 on the nomination of the Mersey Docks and Harbour Company	Superintendent	Inspector	(b), (d), (e) Art.2(b)
A council constituted under s.2 of the Local Government etc. (Scotland) Act 1994	Fire Control Officer	—	(g)
Any fire and rescue authority under the Fire and Rescue Services Act 2004(12)	Fire Control Officer	—	(g)
The Fire Authority for Northern Ireland	Fire Control Officer	—	(g)
A joint fire and rescue board constituted by an amalgamation scheme under s.2 of the Fire (Scotland) Act 2005 or a joint fire and rescue board within the meaning of s.5 of that Act	Fire Control Officer	—	(g)

A National Health Service Trust established under s.5 of the National Health Service and Community Care Act 1990 whose functions, as specified in its Establishment Order, include the provision of emergency ambulance services	Duty Manager of Ambulance Trust Control Rooms	—	(g)
The Northern Ireland Ambulance Service Health and Social Services Trust	Control Supervisor, Ambulance Control Room	—	(g)
The Scottish Ambulance Service Board	Emergency Medical Dispatch Centre Officer In Charge	—	(g)
The Welsh Ambulance Services National Health Service Trust	Regional Control Manager	—	(g)
The Criminal Cases Review Commission	An Investigations Adviser	—	Art.2(a)
The Scottish Criminal Cases Review Commission	A Legal Officer	—	Art.2(a)
The Financial Services Authority	Head of Department, Enforcement Division	—	(b)
The Gambling Commission	Head of Department	—	(b)
The Gangmasters Licensing Authority	Head of Operations	—	(b)
The Information Commissioner	Head of Enforcement	—	(b)
The Independent Police Complaints Commission	Commissioner or Director	—	(b) Art. 2(b)
The Office of Communications	Senior Associate resp. for spectrum investigation technology support	—	(b)
The Office of the Police Ombudsman for Northern Ireland	Senior Investigating Officer	—	(b)
The Royal Mail Group Ltd, by virtue of being a Universal Service Provider within the meaning of the Postal Services Act 2000	Senior Investigation Manager	—	(b)
The Serious Fraud Office	Grade 6	—	(b)

Section 3. Individuals in additional bodies authorised under s.25(1)(g) RIPA by Regulation of Investigatory Powers (Communications Data) Order 2010 that may only acquire communications data falling within s.21(4) (b) and (c) of RIPA	**Prescribed offices (Authorisations/notices relating to communications data falling within s.21(4)(b) and (c) RIPA).**	**Additional prescribed offices: s.21(4)(c) communications data only**	**Reason under s.22(2) RIPA or Art.2 2010 Order**
The Child Maintenance and Enforcement Commission	Senior Executive Officer or equivalent grade	—	(b)
The Department of Agriculture and Rural Development	Head of Financial Policy and Investigations Services	—	(b)
The Department of Enterprise, Trade and Investment	Deputy Chief Inspector in Trading Standards Service	—	(b)
The Department for Business, Innovation and Skills	Deputy Chief Investigation Officer in the Investigation Officers Branch	—	(b)
The Department of the Environment	Principal Grade 7 in the N. Ireland Environment Agency	—	(b), (e)
The Department for Environment, Food and Rural Affairs	Senior Investigation Officer, DEFRA Investigation Services	—	(b)
	Senior Fish Health Inspector (PB6 or above), Centre for Environment, Fisheries and Aquaculture Science	—	(b)
	Deputy Chief Inspector in Marine and Fisheries Agency	—	(b)
The Department of Health	Grade 7 in the Medicines and Healthcare Products Regulatory Agency	—	(b), (d), (e)
The Department for Transport	Head of Enforcement in the Maritime and Coastguard Agency	Enforcement Officer, Maritime & Coastguard Agency	(b), (d)
The Home Office	Immigration Inspector with responsibility for asylum fraud investigations in the UK Border Agency	—	(b)
The Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, a county council in England or Wales, a county borough council in Wales, a district council in England or N. Ireland and a London borough council	Director, Head of Service, Service Manager or equivalent	—	(b)
A council constituted under s.2 of the Local Government etc. (Scotland) Act 1994	Director, Head of Service, Service Manager or equivalent	—	(b)
Any fire and rescue authority under the Fire and Rescue Services Act 2004	Principal Fire Control Officer or Group Manager	—	(b), (d)
The Fire Authority for Northern Ireland	Principal Fire Control Officer or Group Manager	—	(b), (d)
A joint fire and rescue board constituted by an amalgamation	Principal Fire Control Officer or Group Manager	—	(b), (d)

scheme under s.2 of the Fire (Scotland) Act 2005 or a joint fire and rescue board within the meaning of s.5 of that Act			
A National Health Service Trust established under s.5 of the National Health Service and Community Care Act 1990 whose functions, as specified in its Establishment Order, include the provision of emergency ambulance services	Director of Operations or Control and Communications Manager	—	(b)
The Northern Ireland Ambulance Service Health and Social Services Trust	Director of Operations	—	(b)
The Scottish Ambulance Service Board	Director of Operations	—	(b)
The Welsh Ambulance Service National Health Service Trust	Director of Operations	—	(b)
The Charity Commission	Senior Investigations Manager	—	(b)
The Environment Agency	Area Management Team member	—	(b), (d), (e)
The Food Standards Agency	Deputy Director of Legal Services or any Director	—	(b), (e)
The Health and Safety Executive	Band 2 Inspector	—	(b), (d), (e)
The Common Services Agency for the Scottish Health Service	Head of NHS Scotland Counter Fraud Services	—	(b)
The National Health Service Business Services Authority	Senior Manager (not below the grade of Agenda for Change pay band 8b), Counter Fraud and Security Management Services Division	—	(b)
The Northern Ireland Health and Social Services Central Services Agency	Head of the Counter Fraud Unit	—	(b)
The Office of Fair Trading	Any member of the Senior Civil Service with responsibility for cartels or criminal enforcement	—	(b)
The Pensions Regulator	Regulatory Manager	—	(b)
The Scottish Environment Protection Agency	Any Director	—	(b), (d), (e)

Individuals in additional bodies authorised under s.25(1)(g) RIPA by Regulation of Investigatory Powers (Communications Data) Order 2010 that may only acquire communications data within section 21(4) of RIPA relating to a postal service	**Prescribed offices etc (All authorisations/notices relating to communications data relating to postal services**	**Reason under s.22(2) RIPA**
Postal Services Commission	Legal Adviser	(b)

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)?

There are no specific requirements contained within the RIPA 2000 or secondary legislation. There is a Code of Practice drawn up under s.71 of the Regulation of Investigatory Powers Act 2000, *Acquisition and Disclosure of Communications Data: Code of Practice*.[34] It notes that:

> 2.1 The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.
>
> …
>
> 2.5 The designated person must believe that the conduct required by any authorisation or notice is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communication data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.
>
> 2.6 Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to a meaningful degree of collateral intrusion.
>
> 2.7 Taking all these considerations into account in a particular case, an interference with the right to respect of individual privacy may still not be justified because the adverse impact on the privacy of an individual or group of individuals is too severe.
>
> 2.8 Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate.

---

[34] Home Office, *Acquisition and Disclosure of Communications Data: Code of Practice*, London: TSO 2007. Brought into force by The Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2007 (2007 SI No.2197).

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?

There is currently no requirement to obtain a court order before accessing retained data. Nor is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before 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 individuals whose communications data had been subject of a disclosure requirement was discussed during the government consultation on Access to Communications Data. Representations were made that such notification would reassure the public about the use made of powers to acquire communications data and would discourage abuse of powers by officials of public authorities. However, there is no legal requirement to notify under the DRR or RIPA.

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

There is no legal requirement to be informed about the data accessed under the DRR or RIPA. An aggrieved party could make a subject access request to the public authority under the Data Protection Act 1998. The response to this would then be determined subject to appropriate exemptions in the DPA 1998. If this is not successful, then a party may be able to appeal to the Information Tribunal.

> 7.4 There is no provision in [RIPA 2000] preventing [Communications Service Providers] from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.
>
> 7.5 Section 28 provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.
>
> 7.6 Section 29 provides that personal data processed for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.
>
> 7.7 The exercise of the exemption to subject access rights possible under section 29 does not automatically apply to notices given under the Act. In

the event that a CSP receives a subject access request where the fact of a disclosure under the Act might itself be disclosed the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the notice would be likely to prejudice the prevention or detection of crime.[35]

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?

Oversight of access to communications data is via the Interception of Communications Commissioner (appointed under s.57 RIPA) whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of the Act. Any person who uses the powers conferred by Chapter II, or on whom duties are conferred, must comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.[36]

RIPA also established the Investigatory Powers Tribunal (s.65 RIPA). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. It has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under the Act.[37]

If the Commissioner establishes that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

The Tribunal's function is to consider that any conduct covered by RIPA has been properly authorised and carried out in accordance with appropriate guidelines. It can not give a "yes or no" answer as to whether a person is under surveillance or the subject of intelligence targeting.[38]

---

35 *Acquisition and Disclosure of Communications Data: Code of Practice*, 53-54.

36 *Acquisition and Disclosure of Communications Data: Code of Practice*, 58.

37 Ibid, 60.

38 The Investigatory Powers Tribunal: limitations
http://www.ipt-uk.com/default.asp?sectionID=2

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.

According to the RIPA Code of Practice, all (not just personal data) communications data acquired or obtained under the provisions of the Act, and all copies, extracts and summaries of it, must be handled and stored securely. As much communications data will be personal data, however, this is likely to have little practical effect. The requirements of the Data Protection Act 1998 and its data protection principles must also be adhered to under the Code of Practice.[39] The DRR states at Reg. 6 that:

> 6.—(1) Public communications providers must observe the following principles with respect to data retained in accordance with these Regulations—
>
> (a) the retained data must be of the same quality and subject to the same security and protection as those data on the public electronic communications network;
>
> (b) the data must be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
>
> (c) the data must be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;
>
> (d) except in the case of data lawfully accessed and preserved, the data retained solely in accordance with these Regulations must be destroyed at the end of the retention period.
>
> (2) It is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of these Regulations with respect to the security of stored data.
>
> (3) As regards the destruction of data at the end of the retention period—
>
> (a) the duty of a public communications provider is to delete the data in such a way as to make access to the data impossible; and
>
> (b) it is sufficient for a public communications provider to make arrangements for the operation of so deleting data to take place at such monthly or shorter intervals as appear to the provider to be convenient.

---

39 *Acquisition and Disclosure of Communications Data: Code of Practice*, 53.

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

Both DRR and RIPA are silent on destruction of retained data accessed by public authorities. Where the retained data is personal data, the Data Protection Act 1998 will govern, and destruction will take place when the purpose for which the data was processed has elapsed.

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.

In principle the obligation on private parties to retain data is very broad. Reg.3 of the DRR states that:

> 3. These Regulations apply to communications data if, or to the extent that, the data are generated or processed in the United Kingdom by public communications providers in the process of supplying the communications services concerned.

However, in practice, the obligation is seems to be interpreted more narrowly. Reg 10 DDR states:

> 10.—(1) These Regulations do not apply to a public communications provider unless the provider is given a notice in writing by the Secretary of State in accordance with this regulation.
>
> (2) The Secretary of State must give a written notice to a public communications provider under paragraph (1) unless the communications data concerned are retained in the United Kingdom in accordance with these Regulations by another public communications provider.
>
> (3) Any such notice must specify—
>
> (a) the public communications provider, or category of public communications providers, to whom it is given, and
>
> (b) the extent to which, and the date from which, the provisions of these Regulations are to apply.
>
> (4) The notice must be given or published in a manner the Secretary of State considers appropriate for bringing it to the attention of the public communications provider, or the category of providers, to whom it given.
>
> (5) It is the duty of a public communications provider to whom a notice is given under this regulation to comply with it.
>
> (6) That duty is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988(4), or for any other appropriate relief.

It is worth noting the link between Reg.10(1) and Reg10(2), the DRR do not apply to a public communications provider unless the provider is given a notice in writing by the Secretary of State, but the Secretary of State must give a written notice to a public communications provider under Reg.10(1) unless the communications data concerned are retained in the UK in accordance with the DRR by another public communications provider, e.g. "resellers of telecommunications' services will not be obliged to collect and retain communications data which are retained by the network operators." [40]

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 practical implication of the answer to Q23 above is that the UK government intends to utilise higher tier providers, via written notice, to collect communications data from smaller reseller networks who will not receive written notices.

In late 2009 the UK government refused to provide:

- the Names of the Public Communications Providers

and / or the

- the Categories of Public Communications Providers

to which the Secretary of State has given a Written Notice, bringing them under the mandatory Communications Data Retention scheme under Reg. 10 of the DRR, via an information request under the UK Freedom of Information Act 2000. The Home Office cited exemptions under s31(1) and (2) and FOIA 2000

> s.31(1) & (2) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would likely to, prejudice-
>
> (1)(a) the prevention or detection of crime
>
> (1)(b) the apprehension or prosecution of offenders
>
> ...
>
> (1)(e) the operation of the immigration controls.
>
> ...
>
> (2)(a) the purpose of ascertaining whether any person has failed to comply with the law.
>
> s.43(2) - Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it).

---

[40] Richard Jones, 'UK Data Retention Regulations' (2008) 24(2) *Computer Law & Security Report*, 147.

An appeal to the Information Commisioner has resulted in the ICO upholding the UK government's decision to withhold the information.[41]

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?

This is difficult to answer with any accuracy given the range of potentially obligated parties. Some of the data will be retained for billing and business purposes (e.g. location based services) as permitted by the:

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003 No. 2426)
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Equally, prior to the 2007 and 2099 DRR, the UK was already operating a voluntary system of data retention of communications traffic data through the Code of Practice for Voluntary Retention of Communications. See Q.45 below.

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)?

No.

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)?

Impossible to quantify accurately. The UK government gave figures for the period 2004-2008.[42] Payments under s.106 ATCSA 2001 commenced after the first code of practice for the retention of communications data was approved by Parliament in 2003, and the first payments were made in financial year 2004. In October 2007, the Data Retention (EC Directive) Regulations 2007 came into force and payments were also made under those regulations.

---

41 Decision Notice: Freedom of Information Act 2000 (Section 50), Reference: FS50259480, 15 November 2010.

http://www.ico.gov.uk/tools_and_resources/decision_notices/~/media/documents/decisionnotices/2010/fs_50259480.ashx

42 See House of Lords, Written answers and statements, HL Deb. July 2008: c231WA

http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80722w0002.htm

Financial year	Grant payments	ATCSA	EUDRD
2004	5	84,582	-
2005	2	770,800	-
2006	4	5,282,100	-
2007	10	5,714,045	2,632,450
2008*	5	2,283,695	1,788,859

* Year to 1 July

The UK Government estimated the cost of the 2009 DRR as £46.5 million and that it would be be cost neutral to the telephone and IT industry.[43] Estimated costs of the Labour Government's Interception Modernisation Programme, which is being revived by the Coalition government, have been put at approximately £2 billion.

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?

Yes. Reg. 11 DRR states:

> 11.—(1) The Secretary of State may reimburse any expenses incurred by a public communications provider in complying with the provisions of these Regulations.
>
> (2) Reimbursement may be conditional on the expenses having been notified to the Secretary of State and agreed in advance.
>
> (3) The Secretary of State may require a public communications provider to comply with any audit that may be reasonably required to monitor a claim for reimbursement.

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

Co-operation between the party retaining the data and the party (public authority) accessing them is governed by the Regulation of Investigatory Powers Act 2000, Chapter 2 - Acquisition and disclosure of communications data s.21-25, and the Code of Practice under under s.71 of the Regulation of Investigatory Powers Act 2000, *Acquisition and Disclosure of Communications Data: Code of Practice*.

---

[43] HC Delegated Legislation Committee, Draft Data Retention (EC Directive) Regulations 2009, 16 March 2009.

http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm

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.

The DRR is silent on the issue of sanctions for infringement of data retention provisions by the obligated parties. The information Commissioner is the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of the DRR with respect to the security of stored data.

The Interception Commissioner oversees the acquisition of communications data under RIPA by public authorities. The Investigatory Powers Tribunal (IPT) investigates complaints of unlawful acquisition of communications data and misuse of such data if acquired under the transposing legislation (DRR/RIPA).[44] The Investigatory Powers Tribunal has the power to provide remedial measures such as destruction of any records held or financial compensation, at the Tribunal's discretion.[45] To date there does not appear to have been a successful (or indeed, any) complaint regarding communications data.[46]

Where there was infringement involving personal data then the provisions of the DPA 1998 would come into play, notably s.13 (civil - compensation of data subject)[47], s.14 (civil - rectification, blocking, erasure or destruction of data)[48], s.55 (criminal offences) and s.55A-E DPA 1998 (administrative penalty).[49]

As such, for example, if an ISP were to retain communications data involving personal data which fell outside the scope of the DRR (e.g. data not covered by the DRR or data for which DRR time limits had expired) and was not permitted to hold it by other legislation, then, barring recourse to conditions or exemptions in the DPA 1998, it would appear to be in breach of the DPA 1998, and thus subject to potential civil and administrative penalties. If a police force acquires communication data retained under

---

44 The Investigatory Powers Tribunal: Communications Data
http://www.ipt-uk.com/default.asp?sectionID=1&chapter=1.5

45 The Investigatory Powers Tribunal: Procedures
http://www.ipt-uk.com/default.asp?sectionID=4

46 The Investigatory Powers Tribunal: IPT Rulings
http://www.ipt-uk.com/default.asp?sectionID=17

47 An individual who suffers damage or distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

48 If a court is satisfied, on the application of a data subject, that they have suffered damage by reason of any contravention by a data controller of any of the requirements o the DPA 1998 in respect of any personal data, in circumstances entitling him to compensation under s.13, and that there is a substantial risk of further contravention in respect of those data in such circumstances,the court may order the rectification, blocking, erasure or destruction of any of those data.

49 The ICO has the power to fine data controllers up to £500, 000 for breaches of the Act.

DRR/RIPA and does not keep it secure, that would breach the DPA 1998. If a police force acquires communication data, retained under DRR/RIPA, unlawfully or misuses it, then recourse would be to the IPT.

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?

Each public authority designated under RIPA 2000 as entitled to access retained data is responsible for making contact with the party retaining the data in order to actually access that data. See s.21-25 RIPA 2000, discussed above.

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?

See answer to question 31.

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?

On the assumption that this question is about data sharing of retained data, the DRR are silent on the issue. RIPA 2000 states at: s.23:

> s.23, RIPA
>
> …
>
> (3)A notice under s.22(4) shall not require the disclosure of data to any person other than—
>
> (a) the person giving the notice; or
>
> (b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice;
>
> but the provisions of the notice shall not specify or otherwise identify a person for the purposes of paragraph (b) unless he holds an office, rank or position with the same relevant public authority as the person giving the notice (subject to subsections (3A) and (3D))
>
> (3A)The provisions of a notice under section 22(4) may specify or otherwise identify a person for the purposes of subsection (3)(b) above if—
>
> (a)the person giving the notice holds an office, rank or position with a police force ("notifying force");

(b)the chief officer of police of the notifying force has made an agreement under section 23(1) of the Police Act 1996 with the chief officer of police of one or more other police forces; and

(c)the person specified in or otherwise identified in the notice holds an office, rank or position with a collaborative force.

(3B)For the purposes of subsection (3A) a police force is a collaborative force if—

(a)its chief officer of police is a party to the agreement mentioned in subsection (3A)(b); and

(b)the persons holding offices, ranks or positions with it are permitted by the terms of the agreement to be specified or otherwise identified in notices under section 22(4) given by a person holding an office, rank or position with the notifying force.

(3C)A reference in subsections (3A) and (3B) to a police force is to the following—

(a)any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London);

(b)the metropolitan police force; and

(c)the City of London police force.

(3D)The provisions of a notice under section 22(4) may also specify or otherwise identify a person for the purposes of subsection (3)(b) above if—

(a)the person giving the notice holds an office, rank or position with a Scottish police force ("Scottish notifying force");

(b)the chief constable of the Scottish notifying force has made an agreement under section 12(1) of the Police (Scotland) Act 1967 with the chief constable of one or more other Scottish police forces; and

(c)the person specified in or otherwise identified in the notice holds an office, rank or position with a collaborative force.

(3E)For the purposes of subsection (3D) a Scottish police force is a collaborative force if—

(a)its chief constable is a party to the agreement mentioned in subsection (3D)(b); and

(b)the persons holding offices, ranks or positions with it are permitted by the terms of the agreement to be specified or otherwise identified in notices under section 22(4) given by a person holding an office, rank or position with the Scottish notifying force.

(3F)A reference in subsections (3D) and (3E) to a Scottish police force is to a police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967.

In other words, when a designated person in a public authority requires a party retaining the data to disclose that data by notice, such disclosure can only be required to be made to a designated person within the public authority in question.

Once the retained data has been lawfully disclosed to a public authority, there are no specific legal rules in place governing co-operation among the different bodies accessing the data and between these and other public authorities. Where the data are personal data, data sharing between public authorities should be permissible if conducted for the purpose for which the data was obtained by the public authority.

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)?

This is outlined in the *Acquisition and Disclosure of Communications Data: Code of Practice.*[50]

Acquisition of communication data on behalf of overseas authorities

…

7.12 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities:

- Judicial co-operation
- Non-judicial co-operation

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

7.13 If the United Kingdom receives a formal request from an overseas court or other prosecuting authority that appears to have a function of making requests for legal assistance, the Secretary of State (in Scotland the Lord Advocate) will consider the request under the Crime (International Co-operation) Act 2003. In order to assist he must be satisfied that the request is made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom.

---

50 *Acquisition and Disclosure of Communications Data: Code of Practice,* 55-57.

7.14 If such a request is accepted, that request will be passed to a nominated court in the United Kingdom. That court may make an order requiring a CSP to disclose the relevant information to the court for onward transmission to the overseas authority.

Non-judicial co-operation

7.15 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of the Act.

7.16 The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.17 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that.83 Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

7.18 If the proposed transfer of data is to an authority within the European Union that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.19 If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway) then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, including Canada and Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.

7.20 In all other circumstances the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. If necessary the Information Commissioner can give guidance.

7.21 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of ‘substantial public interest’ There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a

third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis.

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)?

As per Q20 oversight of access to communications data is via the Interception of Communications Commissioner (appointed under s.57 RIPA) whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of the Act. Any person who uses the powers conferred by Chapter II, or on whom duties are conferred, must comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

s.57 RIPA: Interception of Communications Commissioner.

(1) The Prime Minister shall appoint a Commissioner to be known as the Interception of Communications Commissioner.

(2) Subject to subsection (4), the Interception of Communications Commissioner shall keep under review—

...

(b)the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I;

...

(3) The Interception of Communications Commissioner shall give the Tribunal all such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require—

(a) in connection with the investigation of any matter by the Tribunal; or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.

(4)It shall not be the function of the Interception of Communications Commissioner to keep under review the exercise of any power of the Secretary of State to make, amend or revoke any subordinate legislation.

(5) A person shall not be appointed under this section as the Interception of Communications Commissioner unless he holds or has held a high judicial office (within the meaning of [F185Part 3 of the Constitutional Reform Act 2005) or is or has been a member of the Judicial Committee of the Privy Council]).

(6) The Interception of Communications Commissioner shall hold office in accordance with the terms of his appointment; and there shall be paid to him out of money provided by Parliament such allowances as the Treasury may determine.

(7) The Secretary of State, after consultation with the Interception of Communications Commissioner, shall—

(a) make such technical facilities available to the Commissioner, and

(b) subject to the approval of the Treasury as to numbers, provide the Commissioner with such staff,

as are sufficient to secure that the Commissioner is able properly to carry out his functions.

RIPA also established the Investigatory Powers Tribunal (s.65 RIPA). The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. It has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under the Act.

65 The Tribunal.

(1) There shall, for the purpose of exercising the jurisdiction conferred on them by this section, be a tribunal consisting of such number of members as Her Majesty may by Letters Patent appoint.

(2)The jurisdiction of the Tribunal shall be—

(a) to be the only appropriate tribunal for the purposes of s.7 of the Human Rights Act 1998 in relation to any proceedings under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights) which fall within subsection (3) of this section;

(b) to consider and determine any complaints made to them which, in accordance with subsection (4), are complaints for which the Tribunal is the appropriate forum;

...

(d) to hear and determine any other such proceedings falling within subsection (3) as may be allocated to them in accordance with provision made by the Secretary of State by order.

(3) Proceedings fall within this subsection if—

...

(d) they are proceedings relating to the taking place in any challengeable circumstances of any conduct falling within subsection (5).

(4) The Tribunal is the appropriate forum for any complaint if it is a complaint by a person who is aggrieved by any conduct falling within subsection (5) which he believes—

(a) to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any postal service, telecommunications service or telecommunication system; and

(b) to have taken place in challengeable circumstances or to have been carried out by or on behalf of any of the intelligence services.

(5) Subject to subsection (6), conduct falls within this subsection if (whenever it occurred) it is—

...

(c) conduct to which Chapter II of Part I applies;

...

(7) For the purposes of this section conduct takes place in challengeable circumstances if—

(a) it takes place with the authority, or purported authority, of anything falling within subsection (8); or

(b) the circumstances are such that (whether or not there is such authority) it would not have been appropriate for the conduct to take place without it, or at least without proper consideration having been given to whether such authority should be sought;

but conduct does not take place in challengeable circumstances to the extent that it is authorised by, or takes place with the permission of, a judicial authority.

...

(8)The following fall within this subsection—

...

(b) an authorisation or notice under Chapter II of Part I of this Act;

...

As per Q21 it is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of the DRR with respect to the security of stored data.

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?

No

If so, please answer to the following questions:

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

N/A

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

N/A

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?**

N/A

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)?

No

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?

Don't know. See answer to Q24. It is likely, given the funding arrangements in place, that data is stored at the service providers' premises.

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?

Don't know. See answer to Q24. In principle, if the DPA 1998 and Reg.6 DRR are complied with, then data could be stored outside the country

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

a) **no data are retained beyond what is permitted?**

Don't know. See answer to Q24.

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)?

A court order is not required. I know of no such technical interfaces.

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

Don't know. See answer to Q24.

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.

Don't know. See answer to Q24.

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

Don't know. See answer to Q24.

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)?

Don't know. See answer to Q24.

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

Don't know. See answer to Q24.

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)?

Don't know. See answer to Q24.

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?

Don't know. See answer to Q24.

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.

Don't know. See answer to Q24.

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?

Don't know. See answer to Q24.

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).

In the UK, public surveillance measures have rarely been far from the news in the last 10 years, whether the issue is the use of CCTV cameras; Automatic Number Plate Recognition; databases such as the national DNA Database, ContactPoint, the National Identity Register, and eBorders; biometric passports; identity cards; or data retention. Citizens are often mistrustful of government surveillance initiatives because they believe either that data collected will be used for purposes other than which it was originally collected ('feature creep' being a common element of UK public surveillance measures), or that the government is not capable of maintaining adequate measures against misuse or loss of data.

The last Labour Government (1997–2010) was perceived as being particularly intrusive, and the incoming Coalition Government (2010-) sought, during the election, to differentiate itself from the previous government's policies by promising to abolish certain databases and public surveillance measures. However, the recent trend in the UK towards greater public surveillance is unlikely to be stopped in its tracks, and it is unlikely that measures such as the DDRs will see significant reform in the near future. Indeed, it is clear that the new government is still keen on measures initiated by its predecessor such as permitting greater data sharing between public authorities, and seeking to retain communication data from a wider variety of Information Society Services.

Data retention has not seen the same type of negative response from the public as the proposed Identity Card or DNA database, this is probably because:

- data retention in the telecoms area was effectively in place prior to the passage of the Directive;
- the public do not appear to perceive data retention to be as significant/emotive an issue as, for example, use of biometrics;
- the public has become increasingly desensitised to potentially privacy invasive public surveillance measures, apathetic in their opposition to them, and cynical about the effectiveness of safeguards/watchdogs like the ICO.

The key issue the public tends to have with data retention is not so much that retention occurs; rather it is with the number and nature of the public authorities who are allowed to access it. Under RIPA 2000 and subsequent secondary legislation the number of public authorities able to access some or all types of communications data has significantly increased. While the general public are not generally unsympathetic to the idea that communications data should be retained for the purposes of tackling serious crime or terrorism, it is clear that their tolerance for more general use of such data is more limited.

In general though, public-oriented opposition to data retention has tended to come from vocal privacy activist groups, such as Privacy International, Open Rights Group, and the Foundation for Information Policy Research or from anti-EU groups, opposed in principle to EU legislation.

Unsurprisingly, there has been significant opposition to data retention requirements from potentially affected commercial organisations such as telecoms providers and ISPs. However, this opposition has become more muted as the government has indicated it is willing to:

- operate data retention primarily through higher tier providers, such as BT, and not to place significant regulatory burden on smaller commercial players;
- provide sufficient compensation to make data retention for the higher tier providers close to cost neutral.

How far the latter promise will be carried through in the current adverse economic and political climate remains to be seen.

Prior to the 2007 and 2099 DRR, the UK was already operating a voluntary system of data retention of communications traffic data through the Code of Practice for Voluntary Retention of Communications.[51] The Code was provided for in Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001), and came into force in January 2004.

Although the Code was, in principle, a voluntary system, there was considerable pressure on the telecommunications industry to introduce a scheme, following September 11th 2001, under the threat from the Government of a mandatory scheme being imposed. The Code was unpopular with communications providers, partly

---

[51] See further Edgar A. Whitley and Ian Hosein, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29(11) *Telecommunications Policy* 857.

because of industry concern that compliance with a voluntary code – as opposed to a legal obligation – could breach human rights and data protection legislation; and partly because of concerns about the expense attached to developing permanent retention processes. However, the Home Office indicated that if the voluntary code of practice was not effective then they would make the code compulsory through a statutory instrument.

In principle, the ATSCA 2001 applied to all communications networks. However, the Code only applied to communication service providers who provided a public telecommunications service in the United Kingdom, as defined in s.2 RIPA, and who retained communications data in line with the provisions of the ATCSA 2001. The Code was thus not intended to apply to individuals and organisations that did not provide a public service (e.g. corporate telecommunications and computer networks).

The Code did not require telecommunications service providers and Internet service providers to retain communications data, but it was designed to:

- suggest agreed time periods for retention of certain types of communications data, and;
- where those time periods for retention were longer than the period for which a relevant organisation would normally retain data for business purposes, to provide a basis upon which they might legitimately continue to retain that data for national security purposes and the prevention or detection of crime or the prosecution of offenders relating to the national security.

Like the 2007 and 2009 DRR the Code was also not concerned with the powers of public authorities, such as the police, to obtain communications data retained in line with its guidance. This was, and is, dealt with by Chapter II of Part I of RIPA 2000.

The Code did not require that service providers collect any information that they would not otherwise collect in the course of their business activities. Retention periods for traffic data were deemed to begin at the point when a communications ended, e.g. when a telephone caller hung up; for service usage data at the completion of a use, e.g. following a mobile phone service transaction; and for subscriber-related data, when the data changed or when the subscriber left the service.

The maximum retention period for communications data held under the Code was 12 months. However, if the communication service provider's business practices required a longer retention period, the Code did not prevent this.

The Code also provided that the Home Office could enter into more detailed service level agreements with individual communication service providers who receive requests for communications data stored under its provisions. As such arrangements carried financial overheads, the government would make payments to communication service providers to cover these retention costs in certain circumstances, e.g. where data retention periods were significantly longer for national security purposes than for business purposes. Agreements were voluntary and could be terminated by either party

subject to an agreed period of notice.[52] The Voluntary Code was replaced for fixed network telephony and mobile telephony communications providers by the 2007 DRR and for internet access, internet e-mail or internet telephony by the 2009 DRR.

The government has consulted widely on the issue of data retention over the last 7 years, see for example:

- Home Office, Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data, Mar. 2003.
  http://www.statewatch.org/news/2003/mar/atcs.pdf
- Home Office, Access to communications data – respecting privacy and protecting the public from crime: Consultation Paper, Mar. 2003.
  http://www.statewatch.org/news/2003/mar/ripa.pdf
- Home Office, Consultation on the initial transposition of the European Directive (2006/24/EC) on the retention of communications data, Mar. 2007
  http://www.statewatch.org/news/2007/mar/uk-ho-cons-eur-dir-data-ret.pdf
- Home Office, Transposition of Directive 2006/24/EC: Consultation Paper, Aug. 2008.
  http://www.statewatch.org/news/2008/aug/uk-ho-consult-mand-ret-internet.pdf
- Home Office, Government Response to the Public Consultation on the Transposition of Directive 2006/24/EC, Feb. 2009.
  http://www.statewatch.org/news/2009/feb/uk-data-ret-consult-response.pdf
- Home Office, Protecting the Public in a Changing Communications Environment: Consultation Paper, Apr. 2009.
  http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf
- Home Office, Protecting the Public in a Changing Communications Environment: Summary of Responses to the 2009 Consultation Paper, Nov. 2009.
  http://www.parliament.uk/deposits/depositedpapers/2009/DEP2009-2754.pdf

Responses to consultations have tended to be from much the same parties each time.

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)?

The following government databases meet, or would have met, the criteria set out above:

- The DNA Database set up under the Criminal Justice and Public Order Act 1994 s.54-58[53] and Criminal Justice Act 2003 s.9-10,[54] and considered by the

---

52 An example of such an agreement being reached by the Government was reported in *The Financial Times* (p.4, 11 November 2005). The Government reportedly paid £875 000 to cover mobile operator O^2's data retention costs, and to provide a system capable of retrieving the type of specific information likely to be requested by law enforcement agencies.

53 http://www.opsi.gov.uk/acts/acts1994/ukpga_19940033_en_1

54 http://www.opsi.gov.uk/acts/acts2003/ukpga_20030044_en_1

ECHR in S. *and Marper v. United Kingdom*.[55] This permits the police to take and retain DNA samples from all individuals who are arrested, regardless of whether they are charged with or convicted of a crime. The ECourtHR held that holding the DNA of those not convicted of a crime was a breach of Art. 8 ECHR – the UK government is still debating how to change the law.

- The eBorders database[56] set up under the Immigration Act 1971 paras. 27 and 27B of Schedule 2 as amended in 2006[57] and s.32-38 of the Immigration, Asylum and Nationality Act 2006[58] and via the following secondary legislation:
    - the Immigration, Asylum and Nationality Act 2006 (Commencement No 7) Order 2007 (statutory instrument 2007 No 3138 as amended by statutory instrument 2007 No 3580);
    - the Channel Tunnel (International Arrangements and Miscellaneous Provisions) (Amendment) Order 2007 (statutory instrument 2007 No 3579);
    - the Immigration and Police (Passenger, Crew and Service Information) Order 2008 (statutory instrument 2008 No 5);
    - the Immigration, Asylum and Nationality Act 2006 (Duty to Share Information and Disclosure of Information for Security Purposes) Order 2008 (statutory instrument 2008 No 539);
    - and the Immigration, Asylum and Nationality Act 2006 (Data Sharing Code of Practice) Order 2008 (statutory instrument 2008 No 8).

This "creates powers for the UK Border Agency and the police to obtain passenger, crew and service data from carriers in advance of all movements into and out of the United Kingdom and a duty for the border agencies to share that data among themselves." Data collected includes:

- mandatory data, which must be collected and supplied when requested at particular time, e.g. for passengers for passengers, the travel document information (TDI) which are the data held in the machine readable zone of the passport or identity document.
- additional data which must be supplied only to the extent which the carrier knows the data, e.g. passenger name record data (PNR) - details collected for a carrier's own commercial purposes - including details

---

55 S. and Marper v. United Kingdom. 30562/04 [2008] ECHR 1581 (4 December 2008), http://www.bailii.org/eu/cases/ECHR/2008/1581.html

56 Home Office UK Border Agency - e-Borders

http://www.ukba.homeoffice.gov.uk/managingborders/technology/eborders/

http://www.ukba.homeoffice.gov.uk/sitecontent/documents/travel-customs/ebordersoverview

57 http://www.legislation.gov.uk/ukpga/1971/77

58 http://www.legislation.gov.uk/ukpga/2006/13

such as passenger name, address, telephone numbers, ticketing information and travel itinerary.

Border agencies must share data with each other where it is likely to be of use for immigration, HM Revenue & Customs, or police purposes; and may also disclose this information to the security and intelligence agencies, if the information is likely to be of use for security purposes. E-borders is currently operational.[59]

- The ContactPoint database set up under the Children Act 2004 s.12[60] and The Children Act 2004 Information Database (England) Regulations 2007[61] that held information on all children under 18 in England (closed down August 6, 2010)[62]

- The National Identity Register designed to be set up under the Identity Cards Act 2006[63] and set to be cancelled by the Identity Documents Bill.[64]

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.

Not that I know of.

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 know 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?

Yes, the Labour government (1997-2010) planned via its Interception Modernisation Programme to extend the government's capabilities for intercepting and storing communications data. This was the subject of the 2009 Home Office Consultation Paper, *Protecting the Public in a Changing Communications Environment* noted at Q45. The consultation paper followed media reports in 2008 that the government was

---

59 UK Border Agency, Our legal powers to collect and manage information on travellers http://www.ukba.homeoffice.gov.uk/aboutus/workingwithus/transportindustry/ebordersrequires/legalpowers/

60 http://www.opsi.gov.uk/acts/acts2004/ukpga_20040031_en_1

61 http://www.opsi.gov.uk/si/si2007/uksi_20072182_en_1

62 http://www.education.gov.uk/childrenandyoungpeople/safeguardingandsocialworkreform/a0063154/written-ministerial-statement-decommissioning-contactpoint

63 http://www.opsi.gov.uk/acts/acts2006/ukpga_20060015_en_1

64 http://www.publications.parliament.uk/pa/cm201011/cmbills/001/2011001.pdf

planning to collect data on all phone calls, emails, chat room discussions and web-browsing habits as part of the IMP.[65] It was claimed that data would include information not usually gathered by CSPs, such as the recipients of email or instant messaging and other third-party data, which could only be gathered through interception and "deep packet inspection".[66] In the consultation the government sought to allay concerns about a centralised database:

> The Government has no plans for a centralised database for storing all communications data. An approach of this kind would require communications service providers to collect all the data required by the public authorities, and not only the data required for their business needs. All of this communications data would then be passed to, retained in, and retrieved from, a single data store. This could be the most effective technical solution to the challenges we face and would go furthest towards maintaining the current capability; but the Government recognises the privacy implications of a single store of communications data and does not, therefore, intend to pursue this approach.[67]

Instead the government envisaged a scenario where:

> 17 … data required by public authorities to protect the public is collected and retained by the communications service providers. This would include both the data that UK communications service providers already collect for their own business purposes and some additional data, largely relating to communications services provided from overseas providers, referred to in this document as third party data.
>
> 18 The responsibility for collecting and retaining this additional third party data would fall on those communications providers, such as the fixed line, mobile and WiFi operators, who own the network infrastructure.
>
> 19. This approach would ensure that all the relevant data was available to investigators but it would not address the problem of fragmentation. … A further step would be for the communications service providers to process the third party communications data and match it with their own business data where it has elements in common; this would make easier the interpretation of that data if and when it were to be accessed by public authorities.

---

65 Leppard, David. "There's no hiding place as spy HQ plans to see all". *The Sunday Times* October 5, 2008

66 Policy Engagement Network, Information Systems and Innovation Group, LSE, Briefing on the Interception Modernisation Programme, June 2009.

http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

All Party Parliamentary Group on privacy Inquiry into communications data surveillance proposals & the Interception Modernisation Programme Briefing paper, July 2009.

http://privacyappg.org.uk/Documents/appg_IMP_briefing.pdf

67 Home Office, Protecting the Public in a Changing Communications Environment: Consultation Paper, Apr. 2009, 4.

The Home Office published a summary of the public consultation in November 2009 (see Q45 above). This noted that the majority of respondents were against the plans to extend the current data retention requirements,[68] and a significant proportion felt that safeguards proposed were inadequate.[69] However, the government noted that:

> The DRD does not meet all requirements in two respects:
>
> not all communication data is covered in the scope of the Directive, for example communications data relating to web chat; and
>
> increasingly, companies that run the networks have no contractual relationship with the communications service being used. One company might provide the broadband network service, whilst a separate company, which might be based abroad, provides an email account. This is a 'third party' relationship; and the company providing the broadband access has no responsibility under the DRD to retain third party data.[70]

Despite the government's clear intention to carry on with the IMP, as expressed in the summary of the public consultation, no legislative measures were forthcoming between the end of the consultation and the General Election in May 2010. This was largely perceived to be because the cost of such a programme (approx. £2 billion) was prohibitive in the economic climate.

After the May 2010 election, the incoming Coalition government stated in their Coalition Agreement that "We will end the storage of internet and email records without good reason."[71] This was followed by a Home Office strategy document published in July 2010, which stated that the Home office planned between June-November 20010 to:

> Publish proposals for the storage of internet and e-mail records, including introducing legislation if necessary. [72]

However, in October 2010, the Coalition Government's Strategic Defence and Security Review proposed that the government would:

> … introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communication data and to

---

68 Home Office, Protecting the Public in a Changing Communications Environment: Summary of Responses to the 2009 Consultation Paper, Nov. 2009, 9

69 Ibid, 11.

70 Ibid, 12.

71 Cabinet Office, *The Coalition: our programme for government*, May 2010, 11. They also pledged to scrap the ID card scheme, the National Identity register and the ContactPoint database (see Q46 above), and halt the next generation of biometric passports; and ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime.

http://www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf

72 Home Office, *Draft Structural Reform*, Plan July 2010, 9.

http://www.homeoffice.gov.uk/publications/about-us/corporate-publications/structural-reform-plan/pdf-version?view=Binary

> intercept communications within the appropriate legal framework. This programme is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counterterrorism operation and in 95% of all serious organised crime investigations. We will legislate to put in place the necessary regulations and safeguards to ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties.[73]

This suggests that the Interception Modernisation Programme remains very much in play, and that the expansion of data retention to a wider range of communications and communications data is planned in the near future, subject to cost.

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) law74 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The ECHR has been incorporated into UK law via the Human Rights Act 1998. As such Article 8 ECHR is the primary source of fundamental rights protecting privacy, personal data and the secrecy of telecommunications. In the absence of a clear constitutional/legislative right, the UK courts have struggled to derive a coherent common law of privacy from caselaw surrounding confidentiality. While cases such as *Halford v United Kingdom*,[75] have driven UK legislative measures to set

---

73 Cabinet Office, *Securing Britain in an Age of Uncertainty:The Strategic Defence and Security Review*, TSO, Oct. 2010, 44.

http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr

74 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).

75 (1997) 24 E.H.R.R. 523

interception /retention of communications and communications data on a clear statutory footing, it is difficult to say that such measures reflect fundamental rights *per se*.

RIPA 2000 which covers the interception of the contents of a communications in Part I Chapter I is silent on what is considered communications content. There is no constitutional definition of 'communications content.'

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?

It is permitted to limit the exercise of the fundamental rights mentioned for the same criteria as are found in Art. 8(2) ECHR.

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?

Not applicable.

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?

Insofar as I understand the question, an assessment/balance of interests would be carried out in each individual case

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)?

No.

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?

No.

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)?

UK law contains a number of statutory provisions which require private actors to share information with law enforcement agencies and other public bodies, e.g.

- Police (terrorism) – Terrorism Act 2000 s.19 - statutory duty to inform the police of information, including personal information, about terrorist activity
- Police (road traffic offences) - Road Traffic Act 1988 s.172 - statutory duty to provide police with identity of driver in certain circumstances.
- Officers of the Department of Works and Pensions, and Local Authorities (benefit fraud) - Social Security Administration Act 1992: s.110A, s.109B and s.109C
- The eBorders regime (outlined above) places an obligation on carriers and ports to provide certain information to the UK Border Agency and law enforcement agencies.

Generally speaking, however, disclosures to the police are not compulsory except in cases where the private actor is served with a court order requiring information. There is no general rule requiring provision of assistance to police.

The Regulation of Investigatory Powers Act 2000, Part III: Investigation of Electronic Data Protected by Encryption requires private actors to co-operate with law enforcement agencies and others. The Act applies where any encryption-protected information comes into the possession of any person (or is likely to do so):

- via a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property;
- by means of the exercise of any statutory power to intercept communications;
- as a result of having been provided or disclosed in pursuance of any statutory duty or;
- has by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise.[76]

In such circumstances, where permission is granted:

- by court order;
- by warrant;
- by statute;
- or in certain circumstances by the Secretary of State, [77]

---

[76] RIPA, s.49 (1)(a)-(e)

that person can require a third party in possession of an encryption key to disclose that key where it is necessary:

- for the exercise or proper performance by any public authority of any statutory power or statutory duty;
- in the interests of national security;
- for the purpose of preventing or detecting crime; or
- in the interests of the economic well-being of the United Kingdom. [78]

The disclosure requirement must be proportionate to achieve the aims to be achieved by its imposition, and the protected information must not be reasonably accessible by other means.[79]

As such the data retention rule is not unique as regards creating a statutory requirement to provide information to law enforcement authorities and other public authorities.

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

No.

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?

In the UK, the general rule is that international treaties cannot create rights and obligations enforceable in UK courts, unless they have been transformed into national law by an Act of Parliament. The ECHR has been incorporated into UK law via the Human Rights Act 1998. In principle, like any other Act of Parliament in the UK this could be repealed by a future Parliament.

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 It is my considered opinion, and that of our Jean Monnet Professor of EU law at Bristol (who noted in passing that Van Gend en Loos was a claim based on a Treaty article), that the ECJ jurisprudence on direct effect of Directives (i.e. in broad terms, that Directives are capable of vertical direct effect, but not horizontal direct effect) is respected by UK national courts and authorities. Certainly, the UK courts do not

---

77 RIPA, Schedule 2.

78 RIPA, s.49 (2)(b), s.49 (3)

79 RIPA, s.49 (2)(c)-(d)

appear to have had the type of difficulties that, for example, the Conseil d'Etat has had with the principle of direct effect.

Discussion of transposition of a Directive into UK national law can be found in the BERR document, *Transposition guide: how to implement European directives effectively*.[80] In brief, the responsible UK ministry will

- decide the means of transposition, e.g primary legislation, secondary legislation (e.g. a Legislative Reform Order or secondary legislation made under s.2(2) of the European Communities Act 1972. The DRR 2009 were made under the latter powers);
- instruct ministry lawyers to draft secondary legislation or if primary legislation is needed, instruct Parliamentary Counsel;
- if the measure has a significant impact on business, charities or the voluntary sector, or goes beyond the minimum requirements of the directive, obtain clearance from the Panel for Regulatory Accountability;
- where a new civil penalty or criminal offence or provisions for the investigation of offences are created, consult with the Ministry of Justice, Scottish Executive, Northern Ireland Office and the regulators;
- create a Transposition Note which explains how the Government is transposing the main elements of the relevant European directive into UK law.
- proceed with primary legislation, [81] or secondary legislation.[82]

59. 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.

---

80 Department for Business, Enterprise & Regulatory Reform, Transposition guide: how to implement European directives effectively, BERR September 2007. Chapter 3: Implementing a directive in the UK

http://www.berr.gov.uk/files/file44371.pdf

81 House of Commons Information Office, *Parliamentary Stages of a Government Bill*, Factsheet L1 Legislation Series, August 2010

http://www.parliament.uk/documents/commons-information-office/l01.pdf

82 See House of Commons Information Office, *Statutory Instruments* Factsheet L7 Legislative Series (FS No.L7 Ed 3.9) Revised May 2008,

http://www.parliament.uk/documents/commons-information-office/l07.pdf

60. 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?

Powers regarding data retention are granted to the Secretary of State (Home Office) and to the public authorities designated for the purposes of Chapter 2 (acquisition and disclosure of communications data) of Part 1 of RIPA, and in The Regulation of Investigatory Powers (Communications Data) Order 2010.

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

No

IV. Assessment of the overall situation

62. 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?

The UK has a chequered history when it comes to the monitoring of the communications of its citizens. Because of this, there are significant concerns on the part of sections of the public about the scope of data retention that already exists under the DRR 2009, and that which is likely to be proposed as part of the Interception Modernisation Programme or its successor under the Coalition government. Service providers are similarly concerned about the potential cost, and the extent to which such cost will be covered by government funding at a time of significant budgetary cuts.

That having been said, abuses of the RIPA-based system for access to retained data have, thus far, apparently been both rare and relatively minor. Use by local authorities of RIPA powers (not just access to retained data) for relatively minor issues, such as dog fouling, access to education and minor fraud have seen a widespread public backlash, which was reflected in the Coalition government's pledge that they would ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime (see the Protection of Freedoms Bill 2010-11, s.37).[83] A similar approach to the access to retained data across a wider range of bodies who are authorised under RIPA 2000 and Regulation of Investigatory Powers (Communications Data) Order 2010, would in principle, provide a greater check and balance than exists under the current 'self-certification' process. A situation where a senior person within a public authority is authorised to decide whether a request by the public authority is reasonable and proportionate in the circumstances, and takes into account the rights of those whose

---

[83] Protection of Freedoms Bill 2010-11.
http://services.parliament.uk/bills/2010-11/protectionoffreedoms.html

retained data is being accessed, is unlikely to reassure the public about the use made of powers to acquire communications data or discourage abuse of powers by officials of public authorities.

There are are reasonable oversight processes for service providers, in the form of scrutiny by the ICO of data protection and data security measures under Reg.6 DRR, and prescibed reporting procedures to the secretary of sState under Reg.9 DRR. these are combined with scrutiny of the use by public authorities of their powers under RIPA 2000 by the Interception of Communications Commissioner and the Investigatory Powers Tribunal, also including prescribed reporting procedures, and the publication of the Interception of Communications Commissioner's Annual Report which amongst other things, assesses the working of the RIPA communications data access provisions, including reported errors.[84] However, the ability of members of the public to effectively utilise those oversight mechanisms is restricted by the lack of data provided about how and when access to retained data takes place. The fact that there is no obligation upon public authorities to inform citizens that data concerning them has been accessed, even after the need for the access, or for secrecy about the access, has ended, leaves citizens at a significant disadvantage when it comes to identifying and challenging possible abuses of power. It is also a concern that the Government has thus far refused to confirm exactly which communications service providers are covered by notices under Reg.10 DRR, despite requests under the FOAI 2000.

In short, therefore, despite government assurances that processes are in place to ensure that data retention, and access to data retained, are restrained by the requirement that public authorities act in a clear, fair and proportionate manner, there is a large information gap for citizens, which signally impairs their ability to make use of those processes. This type of information gap is a problem that is seen elsewhere in UK law, notably in the area of data protection law, where citizens often do not have the information required to effectively utilise their data protection rights against abusive data controllers and other third parties.

---

[84] e.g. Report of the Interception of Communications Commissioner for 2009, TSO, July 2010, 7-17. http://www.statewatch.org/news/2010/aug/uk-interception-of-telecomms-comm-report-2009.pdf

Proposals for improvement of the current regime

- Disclosure of which Public Communications Providers the Secretary of State has given a Written Notice, bringing them under the mandatory Communications Data Retention scheme under Reg. 10 of the DRR and the nature/content of any Service Level Agreements with Public Communications Providers. The UK government currently refuses to provide this information.

- Disclosure of the information requested in Q38-44 of this questionnaire, which is not, to the best of my knowledge, currently publicly available. The UK government has justified such refusal in the past on the grounds that disclosing this kind of information would impair the effectiveness of investigations, or affect the commercial interests of the Public Communications Providers concerned.

- Individuals should, at a minimum, have the right to be informed that their communications data has been accessed, by whom it has been accessed and for what purpose, once the purpose for which the data was accessed has lapsed, e.g. where data is no longer required for the detection or prevention of crime, or ongoing legal proceedings.

- The fragmentation of responsibility for the oversight of the data retention regime should be addressed, as the current regime lacks clarity and consistency.
    - Oversight of access to communications data via the Interception of Communications Commissioner;
    - Review of the legality of access to, and use of, communications data via the Information Tribunal;
    - Monitoring the application of the provisions of the DRR with respect to the security of stored data via the Information Commission.

  The data retention regime should ideally be subject to judicial oversight, rather than dealt with by a separate Tribunal whose powers are relatively limited, whose processes are opaque and whose decisions are crcumscribed

- Greater consideration needs to be given to the type of authorities who directly, or indirectly (e.g. through data sharing arrangments) have access to communication data obtained through the retention process, the proportionaslity of the purposes for which they have been granted access and the suitability of authorisation and oversight mechanisms. The Protection of Freedoms Bill s.37 (see above Q63) is a small step in the right direction as it would require access to communications data by local authorities to be subject to a magistrate's approval mechanism.

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

United Kingdom

Andrew Charlesworth

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*?

The UK does not have a written constitution. There is no constitutional principle or clear constitutional right to communicate anonymously (or using encryption - see, for example, the Regulation of Investigatory Powers Act 2000 s.49/s.53 and the case of R. v S & A [2008] EWCA Crim 2177, where the appellants were served with notices under s.49 of RIPA, requiring them to disclose the password or keys to the encrypted files, and then charged under s.53 RIPA after refusing to comply, also Greater Manchester Police v Andrews [2011] EWHC 1966).

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?

The Home Office Review of Counter Terrorism and Security Powers was presented to Parliament in late January 2011.

http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/review-findings-and-rec?view=Binary

The Review considered the issue of access to communications data (pp.28-30). It noted that

“There are regulations (the Data Retention Regulations 2009, implementing the EU Data Retention Directive) under which CSPs are required to keep certain types of communications data for longer periods so that public authorities may apply for access to it on a case by case basis. The Anti-Terrorism, Crime and Security Act 2001 (ATCSA) and its Code of Practice also provide for voluntary agreements on the retention of certain communications data by CSPs for purposes relating to national security.“

There was no suggestion that the DRR 2009 required any amendment. Rather the concern was with the range of powers to access data retained under the DRR 2009. This appears to be in line with the responses to the public consultation that occurred prior to the review:

http://www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/sum-responses-to-cons?view=Binary

The Review recommended that

“Government departments, agencies, regulatory authorities and CSPs should be consulted to establish the range of non-RIPA legislative frameworks by which communications data can in principle be acquired from CSPs, and for what purposes. This consultation is currently taking place.

These legal frameworks should then be streamlined to ensure that as far as possible RIPA is the only mechanism by which communications data can be acquired.”

There appears to be little public debate about current data retention legislation in the UK. While the issue has not entirely dropped off the radar, not least because of continuing concerns about policy developments, including the UK government’s Intercept Modernisation Programme, expressed by pressure groups such as the Open Rights Group, it has been overshadowed in terms of public debate by other legislative initatives, most notably the Digital Economy Act 2010. Almost none of the proposals for improvement set out in the response to Q63 of the first questionnaire have agained any traction at all in public debate – the only major concern has been to limit who can have access to retained data, and for what purposes, not the nature and scope of the actual retention itself.

The“quick-freeze” option as an alternative to data retention has received very little attention in open discussion, and appears to have no support politically. I have found only two recent mentions of it, the first in a UK-based e-zine:

http://zine.openrightsgroup.org/comment/2011/the-lives-of-others-%E2%80%93-eu-review-of-the-data-retention-directive

the second in a document hosted by European Digital Rights (EDRi), which it is claimed is a leaked document compiled by representatives of the UK, France and Ireland for a Member States’ "Workshop to consider future options for data retention in the EU" on the 30 June 2011.

http://www.edri.org/files/Data-retention-opinion-Uk-fr-Ie.pdf

The status of the document, who drafted it, and for what purpose, are not possible to identify from the document itself.

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?**

   As far as I am aware, with the exception of some very specific statutory provisions, e.g.

   - Police (terrorism) – Terrorism Act 2000 s.19 - statutory duty to inform the police of information, including personal information, about terrorist activity

   - Police (road traffic offences) - Road Traffic Act 1988 s.172 - statutory duty to provide police with identity of driver in certain circumstances.

   private actors in the UK are usually not obliged to report information of the type specified to law enforcement agencies and other public authorities, unless in receipt of a court order requiring them to do so. Various government agencies have powers to demand information e.g. the Child Support Agency has powers to obtain certain information from, amongst others, the relevant parties, employers and local authorities under the Child Support (Information, Evidence and Disclosure) Regulations 1992; certain officers of the Department of Works and Pensions, and Local Authorities can request information and documents or copies of, or copies of extracts from, such documents as they may reasonably require for the purpose of investigation of benefit fraud under the Social Security Administration Act 1992: s.110A, s.109B and s.109C, but these would appear to fall outside the scope of the question.

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 evidence in court?**

   The right to remain silent/privilege against self-incrimination is recognised in both UK common law and statute and reinforced by Art 6(1) ECHR. It Where the privilege is claimed, the court or judge must be satisfied, in the circumstances of the case and as regards the evidence which the witness is called to give, that it is reasonable to believe that there is real and appreciable hazard to the witness. The right not to incriminate oneself is primarily concerned with respecting the will of a

defendant to remain silent. It does not extend to the use in criminal proceedings of material obtained by compulsion which has an existence independent of the will of the suspect: see, for example, R. v S & A [2008] EWCA Crim 2177 above.

Under UK law, the privilege against self-incrimination would not apply to data that is to be retained and transmitted under the national law transposing Directive 2006/24/EC on data retention, and there is no obvious way that the privilege against self-incrimination under UK law would bar retained data from being retained, transmitted and/or used as evidence in court, as it does not relate to the will of the defendant to remain silent. The retained data clearly has an existence independent of the will of the suspect.

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?

It is not possible to answer the first question, as this information is not publicly accessible. The Code of Practice drawn up under s.71 of the Regulation of Investigatory Powers Act 2000, Acquisition and Disclosure of Communications Data: Code of Practice1 states that:

> 7.1 Communications data acquired or obtained under the provisions of the Act, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998 ('the DPA 1998') and its data protection principles must be adhered to.
>
> 7.2 Communications data ('related communications data') that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in conformity with the duty imposed upon him by the Act.

As such, there appear to be no specific data privacy and data security measures mandated for entitled bodies, beyond those that would usually apply to data that they hold.

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.

The most recent statistics on the use of communications data can be found in the 2010 Annual Report of the Interception of Communications Commissioner2 which was presented to Parliament in June 2011 (pp31-48).

---

1 Home Office, *Acquisition and Disclosure of Communications Data: Code of Practice*, London: TSO 2007. Brought into force by The Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2007 (2007 SI No.2197).

2 HC 1239 SG/2011/117 http://www.ipt-uk.com/docs/Interception_of_Communications_2406.pdf

B. Country-specific questions

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

It appears that the data retention regime imposed by the DDR 2009 in the UK is broadly considered to be 'constitutionally' valid. There has been no challenge to the legality of the Act in the UK, as there has been in several other EU Member States. While one might pursue an Art.8 challenge, it does not seem likely that this would succeed in the current political climate.

8. Do you have any information about how the provisions cited under question 19 of the first questionnaire (7.4 to 7.7 of the Acquisition and Disclosure of Communications Data Code of Practice) are handled in practice? Are subject access requests usually met, or is information frequently denied? Which arguments are brought up by the providers to justify the denial of information? Is there a way for the aggrieved party to obtain the information which data have been accessed by approaching the public body that has requested the data?

I do not know of a successful application under the subject access provisions (s.7) of the DPA 1998 to data retained under the DRR 2009. One slight hitch is that we are technically in ignorance of which PCPs are covered by a Written Notice under the DRR 2009. However, on the assumption that we could make guess that BT, Vodafone and O2 are all covered, in principle one could ask for the communications data held. An immediate problem might be demonstrating that the information requested was necessarily our personal data. In most cases where the data held by a PCP has been accessed by an entitled body, the PCP would be able to refuse access under s.28/s.29 DPA 1998 and it would be hard for a data subject to demonstrate otherwise. I can find no evidence of any challenge to a PCP's refusal to disclose information subsequent to a subject access request, or any reported caselaw.

9. Please describe the applicable rules on reimbursement of costs in detail. Which categories of costs are covered (i.e. is it possible to further narrow down the very broad wording "any expenses")? 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?

Regulation 11 of the DDR 2009 states:

Reimbursement of expenses of compliance

> 11.—(1) The Secretary of State may reimburse any expenses incurred by a public communications provider in complying with the provisions of these Regulations.

(2) Reimbursement may be conditional on the expenses having been notified to the Secretary of State and agreed in advance.

(3) The Secretary of State may require a public communications provider to comply with any audit that may be reasonably required to monitor a claim for reimbursement.

Beyond this the regime for reimbursement of costs is not publicly available. Remember that the government currently will not disclose:

- the Names of the Public Communications Providers

  and / or the

- the Categories of Public Communications Providers

to which the Secretary of State has given a Written Notice, bringing them under the mandatory Communications Data Retention scheme under Reg. 10 of the DRR.[3] It is perhaps not surprising therefore that the government has not made available the applicable rules on reimbursement of costs.

10. Have the technical and organisational measures necessary to implement the legal requirements regarding data security (as set out in your answers to question 21 and 26 of the first questionnaire) been standardised or specified by regulations or administrative guidelines? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.

Not to the best of my knowledge.

In particular: do they provide for measures in one or more of the following areas:

- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**

- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**

- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**

- **access logging**

- **secure (irreversible) deletion after expiry**

---

3 http://www.ico.gov.uk/tools_and_resources/decision_notices/~/media/documents/decisionnotices/2010/fs_50259480.ashx

- **error correction mechanisms (e.g. hash functions, checksums)**

- **secure data transmission (cryptographic security, postal delivery)**

- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**

- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**

- **staff training/internal control mechanisms to ensure compliance with the law and other rules**

- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications)?

Not applicable.

11. **As regards your answer to question 35 of the first questionnaire: are there any public bodies responsible for supervising compliance of the communications providers with the data retention obligations, as far as these obligations do not concern data security? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

The Interception of Communications Commissioner maintains a degree of oversight of the communications providers - see p.28of the 2010 Annual Report of the Interception of Communications Commissioner, which outlines errors made by communications providers and actions taken. Whether the ICC is independent is a moot point - the current ICC, The Rt. Hon. Sir Paul Kennedy "served as a Justice of the High Court, assigned to the Queen's Bench Division, from 1983 to 1992. He was Presiding Judge of the North Eastern Circuit from 1985 to 1989. He served as Lord Justice of Appeal from 1992 to 2005 and also as Vice-President of the Queen's Bench Division from 1997 to 2002." This means that he is a senior judicial appointment and thus one might think likely to be independent, but it also means that he is very much part of the Establishment. The ICC is appointed by the Prime Minister and may be reappointed at the Prime Minister's discretion (s.57 RIPA). Additionally, the Secretary of State for the Home Office, after consultation with the Interception of Communications Commissioner:

- makes such technical facilities available to the Commissioner, and

- subject to the approval of the Treasury as to numbers, provides the Commissioner with such staff,

as are sufficient to secure that the Commissioner is able properly to carry out his functions. So it's arguable that a Commissioner who wants to serve more than one term, and who doesn't want to fight over budget allocations and staff would be wise not to unduly irritate the government of the day.

I apologise for the paucity of material in Q5, 8, 9, 10 – those questions ask for information which I simply don't have access to. I find it very frustrating to have to state that these things are largely off limits to the public.