NETHERLANDS

3.A.1 The primary supervisory authority in the Netherlands on the specific retention obligations of internet access and telecom providers is the ‘Agentschap Telecom’ (Radio Communications Agency). The Dutch data protection authority (College bescherming persoonsgegevens) has a general supervisory authority on the processing of personal data. The two authorities have closed a cooperation covenant, signed on 15 September 2009, detailing their collaboration in the supervision on this specific issue of the sector. The protocol is available at: http://www.cbpweb.nl/downloads_pb/pb_20090915_samenwerkingsovereenkomst_AT-CBP.pdf (in Dutch only).

The Dutch DPA has general administrative investigative powers and specific powers granted by the Dutch data protection act (Wet bescherming persoonsgegevens). All these powers apply equally to the private and the public sector.

The general administrative investigative powers are:
- the power to enter and search business (Article 5:15 of the General Administrative Law Act) and private premises (Article 5:17 General Administrative Law Act), land and means of transport;
- the power to request police assistance; (Article 5:15 of the General Administrative Law Act)
- the power to examine and copy books and business records (Article 5:16 and 5:17 General Administrative Law Act);
- the power to make on-the-spot oral inquiries on business premises (Article 5:16 and 5:17 of the General Administrative Law Act).

The specific investigative powers are:
- the power to launch an investigation by virtue of the office into any processing of personal data or at the request of a data subject (Article 60 of the Dutch data protection act)
- the power to inspect private homes without the occupant’s prior consent (Article 61 of the Dutch data protection act)

It is criminally sanctioned not to co-operate with the investigation (Article 184 of the Criminal Code Act), as well as frustrating the investigation by, for example, making the details of an investigation known to third parties.

The Dutch DPA has not received any complaints about the new data retention act, but has started an investigation as part of a joint enforcement action of all the data protection authorities in the EU, united in the Article 29 Working Party and is closely collaborating with the Radiocommunications Agency on a first investigation into the retention periods and deletion policies in the sector.

In the first investigation, coordinated within the Article 29 Working Party, the Dutch DPA sent (uniform) questions and has conducted on site inspections at 4 companies in the Netherlands in September 2009. The Agency has accompanied the Dutch DPA during the on site inspections at the 4 Dutch companies, to learn more about the working methods of the Dutch DPA.
The deadline for the presentation of Dutch DPA draft report to the plenary meeting of WP29 is mid December 2009. The draft report collating all the national findings is expected to be presented in draft form to the plenary on 1 March 2010.

The second investigation is conducted primarily by the Radio Communications Agency and is a so-called zero-measurement. The Agency has sent out questionnaires to 300 relevant telecommunications providers in the Netherlands, asking for example about the general information security strategy and policy. The Agency will perform a risk-analysis on these results and follow-up in 2010/2011 with more specific investigations into (perceived) high-risk operators.

3.A.2 The investigative powers of the Dutch DPA apply equally to the private and the public sector. The Dutch DPA has not investigated any specific complaints about the new data retention obligations, but, on a related topic, is currently investigating the processing of data by and through the CIOT (Central Information Point for Telecommunication Research). This is a system in which telephone and Internet providers copy the names, addresses and residence details of their customers to a separate server that can be consulted via the CIOT. The competent authorities can query all providers at the same time via the CIOT in order to obtain the identity of the user of a particular number (including e-mail addresses and IP numbers) or, vice versa, the number pertaining to a particular identity. CIOT is an organisation that is part of the Ministry of Justice. The Dutch DPA cannot disclose any details about this investigation during this investigation.

3.A.3. The Dutch DPA has the power to audit the compliance of providers, but given the covenant with the Radiocommunications Agency, it is primarily up to this Agency to audit the compliance.

3.A.4. The Dutch DPA has identified a number of problems with the implementation of the Directive.
1. legal: The Dutch implementation includes location data from mobile phones 'during communication', when they are generated. This type of data was specifically excluded from the European obligation because of the threat of permanent, all encompassing surveillance of all citizens, in violation of article 8 of the European Convention on Human Rights.
2. legal: The Dutch implementation is not specific enough when it comes to the exact type of data that need to be retained. We are aware, for example, of discussions between providers and law enforcement whether providers should also retain the IP address from the connection device of the sender of each incoming mail for their customers.
3. legal: The Dutch implementation does not exclude central storage of the data, but has chosen to temporarily leave it up to the market. The most logical model for central storage is the model already in place of the CIOT, where providers provide a daily upload of the name and number data of their customers. The Dutch DPA has grave concerns about the security and access limitations to such a system when it would include all the historical telecommunications traffic data.
3.A.5. There is no experience that can be disclosed at this moment.

3.A.6 There is no case law yet.

3.B Dutch DPA has not conducted any investigations with regard to the use of prepaid SIM cards. In 1998, when the new Telecommunication Act was discussed in parliament, the Dutch DPA advised parliament about the inappropriateness of "the probably ineffective general registration of all holders of prepaid cards".

In practice, law enforcement authorities have two possibilities to identify and intercept communications of owners of prepaid SIM cards.

- The first is to use fake base stations (IMSI catchers) to intercept all communications in a certain area. This use of the frequency space is legally based on article 3.10, article 4, of the Dutch Telecommunications Act.

- Secondly, since 2002 telecommunications providers are legally obliged to be able to conduct data analysis on location data of mobile phones, by the Decree on Special Collection of Number Data from 2002. Providers are obliged to retain the information required for the data analysis for a period of three months. These data are: the times when telecommunications have taken place, the numbers corresponding with those times and with the relevant telecommunication and the base stations (cells) where the information was received.

The predecessor of the Dutch DPA (called ‘Registratiekamer’) was very critical in its advise to parliament in 1998 about the use of IMSI catchers, since "no legal guarantee is given that with such scanning devices the confidentiality of the communications between not-suspected people is not violated."

In general, a possible obligation to obtain the identify the owners of currently anonymous owners of prepaid cards would involve a huge logistic operation, in which very sensitive data will be processed by many different private parties. If the Dutch DPA would be asked for its advise on such an obligation, it would pay attention to the risks of identity theft/fraud that can be caused by the massive photo copying of identity documents.