Exempt or irrelevant matter deleted (s 22)

Exempt or irrelevant matter deleted (s 22)

Sent: Monday, 14 April 2014 10:52 AM

Exempt or irrelevant matter deleted (s 22)

Subject: D [DLM=For-Official-Use-Only]

For Official Use Only

Exempt or irrelevant matter deleted (s 22)

As discussed on Friday, I am forwarding to you the following documents:

- current approach to data retention (info from a recent senate estimates brief)

Documents affecting national security or defence or international relations (s 33)

- a press release from the Court of Justice of the European Union in relation to its recent decision on the EU Data Retention Directive, and
- talking points that were developed for the Court of Justice of the EU decision.

Documents affecting national security or defence or international relations (s 33)

tatus of mandatory data retention in Australia, the lso the recent EU decision on the EU Data Retention Directive.

We would be happy to look over any relevant briefing / speech input that is prepared on this issue if that would assist.

Let me know if you need anything further.

Regards

Documents affecting national security or defence or international relations (s 33)

HOT TOPIC BRIEF **NSCJ-14**

Inquiry into Comprehensive Revision of the *Telecommunications (Interception and Access) Act 1979*, including Government response to the PJCIS Report

On 24 June 2013, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) handed down its report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The Committee expressed a range of views and made 43 recommendations, including:

- broad support for reforming the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and specific proposals such as creating a single warrant and allowing for attribute interception
- noting that there is a "diversity of views" on data retention regime
- recommending the Government proceed to create a telecommunications security framework, and
- support for the majority of the proposed measures relating to Australian intelligence agencies.

Government is yet to respond to the PJCIS Report. The three elements of the national security reforms, Telecommunications Interception, Telecommunications Sector Security Reforms and Intelligence Agency Reforms are being progressed separately.

On 12 December 2013, the Senate for Legal and Constitutional Affairs Committee agreed to inquire into the revision of the TIA Act with regard to the recommendations of the PJCIS report and the recommendations of a 2008 Australian Law Reform Commission (ALRC) report, *For Your Information: Australian Privacy Law and Practice*. The Committee will report by 10 June 2014. Senator Ludlum will be Chairing this Inquiry.

Key messages

- The department welcomes the Report of the Parliamentary Joint Committee on Intelligence and Security (Committee).
- Government has not yet responded to the Committee's Report.
- The department acknowledges and supports the Committee's recognition of the need for Australia's security and intelligence agencies to be appropriately resourced and to be granted powers, which are often intrusive, to carry out their work.
- The department agrees with the Committee that intrusive powers must always be balanced by appropriate safeguards for the privacy of individuals and the community.
- The department notes that the Committee supported the majority of proposed measures to improve laws relating to Australian intelligence agencies.
- The department notes the Committee's recommendation that a security framework for the telecommunications sector be established to ensure it is robust and resilient and is progressing advice to the Attorney-General relating to this recommendation.
- The department does not want to make any comments about the reform of interception legislation that may pre-empt the new Senate Legal and Constitutional Affairs Committee Inquiry.
- The department is in the process of preparing a detailed submission for the new Inquiry.

TELECOMMUNICATIONS INTERCEPTION REFORM

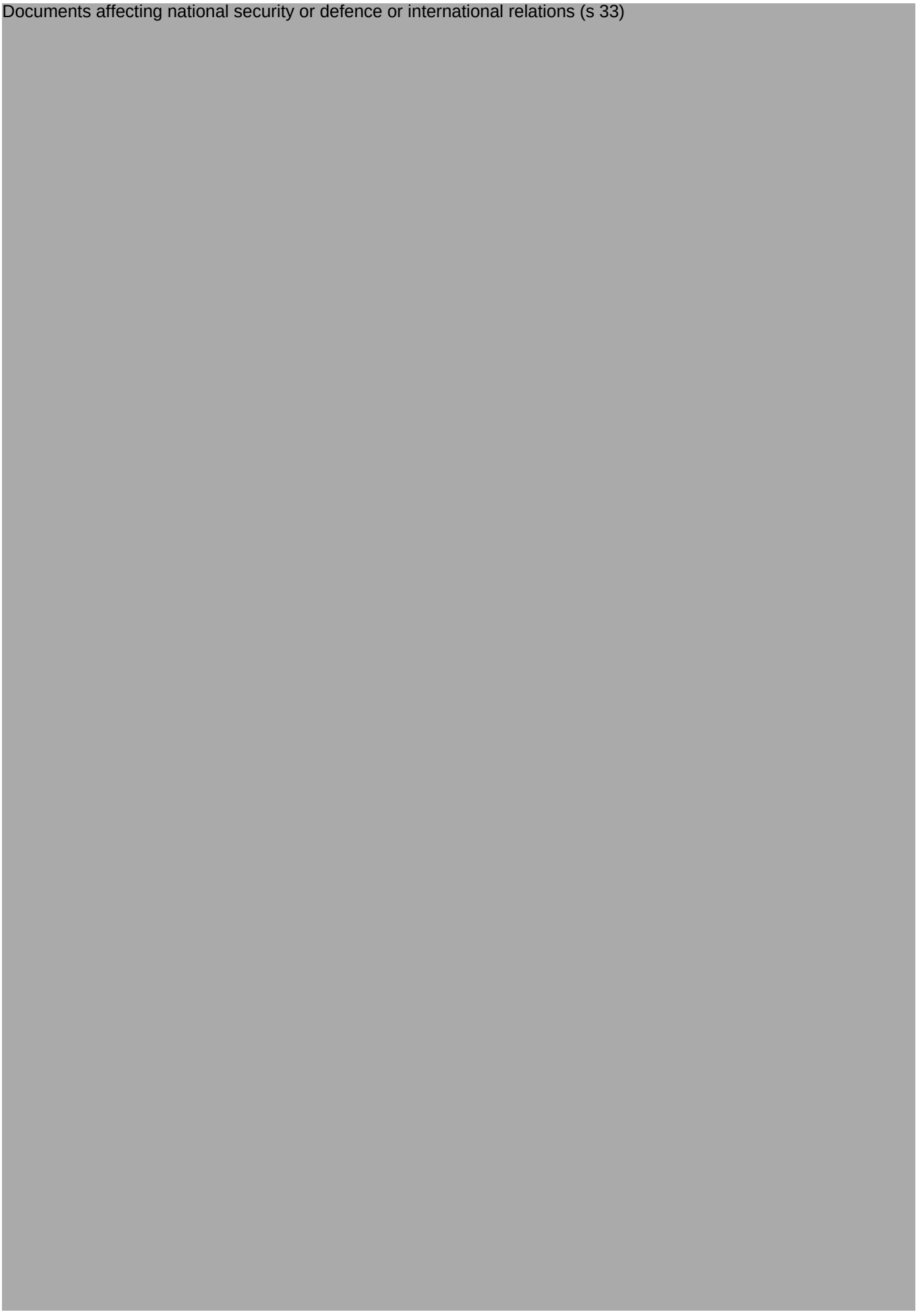
- The Committee was asked to consider proposals seeking to modernise and simplify the 34 year old interception regime and to better assure the privacy of Australians and protect the social and economic wellbeing of the nation.
- The department notes that the Committee supported a holistic review of the legislation as being necessary to ensure the tools and the protections set out in the TI Act reflect the way in which the contemporary communications environment operates.
- No government decisions have been made on progression of the TI reform proposal.
- The department is in the process of preparing a detailed submission to that new Inquiry.

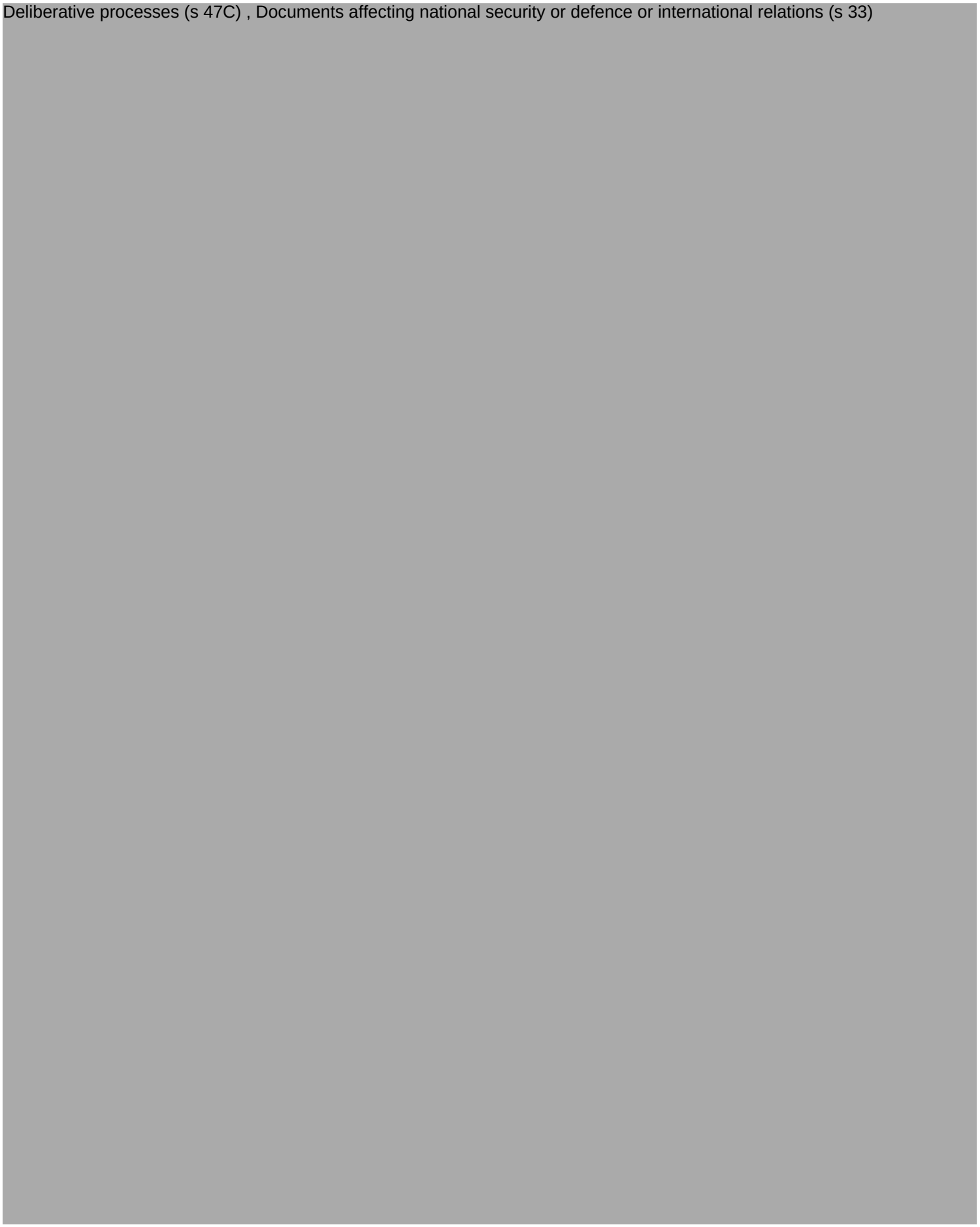
Data retention

- No Government decision has been made about data retention.
- The department acknowledges that there was a diversity of views within the Committee about the mandatory data retention proposal.
- The Committee recommended that, subject to a government decision, an exposure draft of proposed legislation be referred to the Committee for examination.
- The Committee provided guidance on the particulars of any regime, including that internet browsing data should be excluded, the retention period should not be more than 2 years, and that robust oversight, review and reporting arrangements should be put in place.
- Agencies stressed in their evidence to the Committee the importance of data availability to law enforcement and national security capability.
- Data forms an essential part of very many law enforcement and national security investigations.

[If pressed, about the particulars of the need for data retention or the details of data retention]

- The Government has not made a decision on the data retention regime, the Committee's specific guidance on both consultation and the particulars of any regime will be carefully considered before making any decisions.
- The department does not want to make any comments about the reform of interception legislation that may pre-empt the new Senate Legal and Constitutional Affairs Committee Inquiry.
- During their presentation to the Committee, the AFP, NSW and SA Police Commissioners made it very clear that data is fundamentally important to their investigations and that some leads are now failing because carriers are deleting that data more regularly than they have done in the past.
- Data can be used to corroborate a person's identity and address, and can be used to establish relationships between criminals.
- Phone companies retain this information now, but need less data for shorter periods because billing practices are changing.
- Other countries have taken the approach of requiring phone companies to keep certain kinds of data.





Documents affecting national security or defence or international relations (s 33)

CLEARANCE DETAILS

Cleared by: Jamie Lowe, A/g FAS, NSLPD

Exempt or irrelevant matter deleted (s 22)

Court of Justice of the European Union
PRESS RELEASE No 54/14
Luxembourg, 8 April 2014

Press and Information

Judgment in Joined Cases C-293/12 and C-594/12
Digital Rights Ireland and Seitlinger and Others

The Court of Justice declares the Data Retention Directive to be invalid

It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary

The main objective of the Data Retention Directive[1] is to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. It therefore seeks to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. Thus, the directive provides that the abovementioned providers must retain traffic and location data as well as related data necessary to identify the subscriber or user. By contrast, it does not permit the retention of the content of the communication or of information consulted.

The High Court (Ireland) and the Verfassungsgerichtshof (Constitutional Court, Austria) are asking the Court of Justice to examine the validity of the directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data.

The High Court must resolve a dispute between the Irish company Digital Rights Ireland and the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. The Verfassungsgerichtshof has before it several constitutional actions brought by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants. Those actions seek the annulment of the national provision which transposes the directive into Austrian law.

By today's judgment, the Court declares the directive invalid[2].

The Court observes first of all that the data to be retained make it possible, in particular, (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.

The Court takes the view that, **by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.** Furthermore, the fact that data are retained and subsequently used without the

[1] 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 (OJ 2006 L 105, p. 54).
[2] Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the directive entered into force.

subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

The Court then examines whether such an interference with the fundamental rights at issue is justified.

It states that **the retention of data** required by the directive **is not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data.** The directive does not permit the acquisition of knowledge of the content of the electronic communications as such and provides that service or network providers must respect certain principles of data protection and data security.

Furthermore, the retention of data for the purpose of their possible transmission to the competent national authorities **genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security.**

However, the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

In that context, the Court observes that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, **the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.**

Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without **any differentiation, limitation or exception** being made in the light of the objective of fighting against serious crime.

Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have **access to the data** and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.

Thirdly, so far as concerns **the data retention period**, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the **risk of abuse** and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

Lastly, the Court states that the directive does **not** require that the data be **retained within the EU.** Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Press contact: Christopher Fretwell ☎ (+352) 4303 3355

Talking Points on the Court of Justice of the European Union's decision on the EU Data Retention Directive.

What developments have there been in the European Union's data retention scheme?

- The European Union Data Retention Directive requires Member States to oblige telecommunications service providers to retain telecommunications data for between six months and two years for the investigation of serious crime.
- The most recent development is that on 8 April 2014, the Court of Justice of the European Union (ECJ) declared the Directive invalid.
- The ECJ said the retained data made it possible to:
    - know the identity of the person with whom a subscriber or registered user has communicated and by what means,
    - identify the time of the communication as well as the place from which that communication took place and
    - know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
- The court said that this interferes with the right to respect for private life and the right to the protection of personal data.
- The court said that the interference was not justified, on the basis that in the EU DRD:
    - telecommunications data is retained without any differentiation, limitation or exception
    - the directive fails to lay down any objective criterion for access to the data
    - there are no objective criteria for differing retention periods
    - there is no protection against the risk of abuse.
- The Department is still considering the decision of the ECJ and its significance for any possible data retention proposal in Australia. It may be that Australia, as a national government, is better placed to directly implement privacy safeguards and objective standards than is possible in the European context, should the government decide to implement data retention.

If asserted that data retention has been found to be unconstitutional

- On 8 April 2014, the Court of Justice of the European Union declared the European Data Retention Directive invalid.
- The Court's reasoning is very important.
- The Court acknowledged that data retention 'genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security'.
    - The Court also acknowledged that telecommunications data is less privacy sensitive than the content of communications.
- However, the Court concluded that the Directive did not contain sufficient safeguards to protect privacy, and so violated the principle of proportionality under EU law.
    - For example, the Court noted that the Directive did not contain any rules requiring data to be physically stored inside the EU.

If asked about the Court's finding that data retention constitutes a 'serious interference' with the right to privacy

- All investigative powers involve intruding on the right to privacy.
- What is important is that appropriate safeguards are in place to ensure that such intrusions are not disproportionate, to prevent abuse, and to protect the security of information.
- The Court acknowledged that data retention 'genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security'.
- However, the Court concluded that the Directive did not contain sufficient safeguards to protect privacy, and so violated the principle of proportionality under EU law.

If asked about the ramifications of the EU decision for any potential Australian data retention regime

- The Government has not made any decisions about whether to implement a data retention scheme in Australia.
- However, in comparison with the EU Data Retention Directive, the PJCIS recommended a range of detailed safeguards that should apply if Government elected to proceed with an Australian data retention regime.
- In our submission, the Department has also proposed additional safeguards that would apply to agencies accessing telecommunications data under the TIA Act, including

- reassessing which agencies may access telecommunications data, and
- strengthening the independent oversight and public reporting requirements.

If asked about the ramifications of the EU decision for existing EU data retention regimes

- Our advice is that the domestic laws of each EU member-State implementing the EU Data Retention Directive are unaffected by the Court's decision.
- We understand that it would be open to the European Parliament to rewrite the Directive to include sufficient safeguards, to bring it into line with the Court's decision.