Tithe an Oireachtais
Houses of the Oireachtas

Tithe an Oireachtais

An Comhchoiste um Dhlí agus Ceart agus Comhionannas

Tuarascáil ar an nGrinnscrúdú Réamhreachtach ar an mBille Cumarsáide (Sonraí a Choimeád)

Eanáir 2018

Houses of the Oireachtas

Joint Committee on Justice and Equality

Report on Pre-Legislative Scrutiny of the Communications (Retention of Data) Bill 2017

January 2018

32/JAE/22

Tithe an Oireachtais

An Comhchoiste um Dhlí agus Ceart agus Comhionannas

Tuarascáil ar an nGrinnscrúdú Réamhreachtach ar an mBille Cumarsáide (Sonraí a Choimeád)

Eanáir 2018

Houses of the Oireachtas

Joint Committee on Justice and Equality

Report on Pre-Legislative Scrutiny of the Communications (Retention of Data) Bill 2017

January 2018

32/JAE/22

Contents

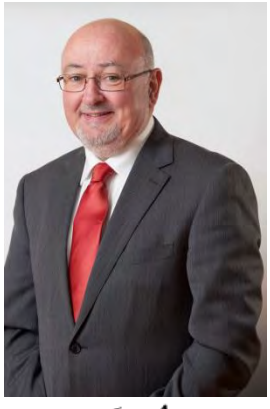
Chairman's Preface

Data protection and data retention are important policy areas which the Oireachtas Joint Committee on Justice and Equality has scrutinised in recent months. Earlier in 2017, the Committee published its *Report on pre-legislative scrutiny of the Data Protection Bill 2017,* which made a number of recommendations to improve the effectiveness of the Bill. The Committee then turned its attention to the General Scheme of the Communications (Retention of Data) Bill 2017 and conducted pre-legislative scrutiny of it.

The Committee held two engagements, in November 2017, with a number of stakeholders to hear a range of views on the General Scheme of the Bill. Data retention is a complex area, and a number of issues and differing viewpoints in relation to the General Scheme emerged in the course of the Committee's deliberations, particularly around journalists and their sources; judicial remedies; and oversight.

The Committee has made a number of recommendations, which can be found at the back of this report, and we very much hope that these will inform the drafting of the final Bill and result in a stronger legislative proposal. A copy of this report and its recommendations has been sent to the Minister for Justice and Equality, and the Committee looks forward to working proactively with the Minister in progressing this legislation in the future.

I would like to express my gratitude on behalf of the Committee to all the witnesses who attended our public hearings to give evidence. Finally, I also wish to thank the staff of the Committee Secretariat, and of the Library & Research Service, who assisted in the preparation of this report. Go raibh maith agaibh.



Caoimhghín Ó Caoláin T.D.
Chairman – January 2018

Summary

The Minister for Justice and Equality, Charles Flanagan TD, published the General Scheme of the *Communications (Retention of Data) Bill 2017* on 3 October 2017.[1] The General Scheme proposes measures to replace the *Communications (Retention of Data) Act 2011.*[2] It takes account of recent decisions of the Court of Justice of the European Union in the *Digital Rights Ireland* [3] and *Tele2* [4] cases, and of a review on the State's data retention law and practices undertaken by former Chief Justice John Murray. [5]

The General Scheme provides for:

- the repeal of the Communications (Retention of Data) Act 2011;
- the exclusion from retention of the contents of communications, such as recordings of voice calls or the text and image contents of emails or websites;
- the designation of the An Garda Síochána, Defence Forces, Revenue Commissioners, Garda Síochána Ombudsman Commission (GSOC) and the Competition and Consumer Protection Commission ('CCPC') as the statutory agencies having authority to request access to retained data;
- the retention by telecommunications service providers of information that identifies subscribers for 12 months, and access to it by designated officers of the statutory agencies in connections with specific serious offences;
- traffic and location data to be retained only by order of the Minister for Justice and Equality on foot of an application by the head of one of the statutory agencies;
- access by designated officers to traffic and location data to be conditional on an order of an authorising judge, and to be restricted to purposes relating to certain serious offences;
- access without a judge's order to be permitted only in cases of urgency;
- service providers to keep retained data securely in the EU, and all retained data to be destroyed when proceedings or investigations conclude;
- criminal penalties for service providers that fail to comply with obligations;
- periodic review of the Act's operation by a designated judge;

[1] Text of the General Scheme available here .
[2] Text of the *Communications (Retention of Data) Act 2011* (as amended) available here
[3] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung, Seitlinger, Tscholl and Others*: Joined Cases C-293/12 and C-594/12, judgment of the Grand Chamber of the CJEU available here.
[4] *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson*: Joined cases C-203/15 and C-698/15, judgment of the Grand Chamber of the CJEU available here.
[5] Review of the Law on the Retention of and Access to Communications Data: Report of Mr Justice John L Murray, available here .

- reports of the designated judge and of the statutory authorities to be laid before the Oireachtas; and
- persons who are the subject of or are affected by a disclosure to be notified of that fact, and to have access to the complaints procedure under the *Interception of Postal Packets and Communications Messages (Regulation) Act 1993*.[6]

Summary of key issues

Key issue 1: Journalists and their sources

The terms of reference for the Murray Report specifically referenced the effect of data retention laws on the work of journalists and the confidentiality of their sources. Consideration of these issues form a significant part of the Report, which makes a number of specific recommendations concerning journalists and issues raised by retention of and access to their communication data. However, the General Scheme makes no reference to journalists or their sources and does not address recommendations dealing specifically with them.

The Committee had to consider:

- whether particular provision should be made in the proposed Act for journalists and their sources; if so,
- whether the provisions should reflect the recommendations in the Murray Report or different measures; and
- how 'journalist' and related terms should be defined.

Key issue 2: Statutory bodies and designated officers

The Murray Report recommended a number of safeguarding measures that should apply to statutory bodies authorised to access retained data and their designated officers. Many, but not all, of those recommendations are reflected in the General Scheme.

The Committee had to consider whether:

- there should be an express limit on the number of designated officers in each statutory body (e.g. three designated officers in the CCPC);
- requests to access retained data should be made by way of statutory declaration or affidavit specifying the exact statutory offence or facts justifying the request; and
- legislation should require all personnel involved in requesting access to retained data to receive formal instruction on the importance of proportionality.

[6] Text of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* available here.

Key issue 3: Independent monitoring authority

The Murray Report recommends that service providers be obliged to keep retained data at an appropriate and objectively verifiable standard of security, and that an independent authority be appointed to monitor compliance with those standards.

The Committee had to consider:

- whether the security standards mandated by Heads 12 are appropriate;
- whether retained data should be required to be kept in the State;
- whether an authority should be appointed to monitor compliance with security standards and, if so,
- the powers and resources required for the proper performance of that authority's functions.

Key issue 4: Statutory cohesion and mutual assistance

The Murray Report criticises a lack of clarity in statutory provisions identifying which bodies may be given access to retained data, and the terms upon which they may be given such access.

The Committee had to consider:

- whether express provision should be made for access to retained data in circumstances not addressed in the General Scheme, such as where a request is made under the Criminal Justice (Mutual Assistance) Act, 2008, and
- whether safeguarding provisions of the General Scheme (such as Head 15 (notification of data requests), Head 18 (review by a dedicated judge), Head 21 (reporting) and Head 22 (complaints procedure)) should make provision for all cases where retained data is accessed, whether under the express terms of the General Scheme or otherwise.

Key issue 5: Judicial remedy

The Murray Report recommends that persons whose rights, potentially including fundamental rights, have been affected by wrongful access to retained data should have an appropriate judicial remedy. It notes that this is a principle supported by EU legislation and decisions of the European Court of Human Rights.

The General Scheme proposes a complaint procedure using the Referee mechanism under section 9 of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. Remedies available under this will comprise quashing of a wrongful authorisation or approval to access data, destruction of that data, and reporting the matter to the head of the relevant statutory agency and the judge appointed to monitor the operation of the proposed Act. The Referee's decision is to be final.

The Committee had to consider whether this provides an appropriate remedy for cases where contravention of the proposed Act causes rights, potentially including fundamental rights, to be breached.

Introduction

This report outlines the background to and contents of the General Scheme of the *Communications (Retention of Data) Bill 2017* [7] and highlights key issues the Joint Committee had to consider.

The paper is divided into the following sections:

- **Background** – describing the nature of data retention, applicable EU and Irish legislation, and the effects of recent decisions of the Court of Justice of the EU in the *Digital Rights Ireland* [8] and *Tele2* [9] cases;

- **The Murray Report** – outlining the review of the State's data retention laws carried out by former Chief Justice Murray and the principal recommendations made in his report to the Minister for Justice and Equality;[10]

- **Outline of the General Scheme** – a summary of each of the Heads in the General Scheme**;** and

- **Key Issues** – describing topical issues raised by the General Scheme and the recommendations of the Murray Report.

Background

What is data retention?

'Data retention' in the present context is the practice whereby telecommunications service providers record and hold information related to their subscribers' telephone and internet communications. The purpose of the retention is normally to assist designated authorities – such as police and security services – in the detection, investigation or prevention of crime, disturbance of public order or threats to national security.

An important characteristic of data retention as generally practised is that the contents of communications – for example, the speech of parties to a telephone call or the text content of an email message – are not retained. Instead, service providers retain 'communications data' (also referred to as 'metadata'), which comprises information about communications. This typically includes the names,

[7] Text of the General Scheme available here.
[8] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung, Seitlinger, Tscholl and Others*: Joined Cases C-293/12 and C-594/12, judgment of the Grand Chamber of the CJEU available here.
[9] *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson*: Joined cases C-203/15 and C-698/15, judgment of the Grand Chamber of the CJEU available here.
[10] Review of the Law on the Retention of and Access to Communications Data: Report of Mr Justice John L Murray, available here.

subscriber numbers and locations of the sender and receiver, the date and time of the communication, the volume of data transmitted and similar details.

Similarly to phone 'tapping', data retention raises concerns regarding rights to privacy, expression, political activity and association. Access to communications data can allow an observer to create a detailed outline of a person's personal, social and professional activities and networks, and even of that person's interests and opinions. Because of these concerns, legislation generally imposes controls on the types of communications data that service providers may retain and the period for which it may be held. For the same reasons, the purposes for which authorities may seek access to communications data and the conditions under which they may use it are restricted.[11] Safeguards vary from one country to another but can include the need for prior approval by a judge, limits on the purposes for which access to the data may be sought and the use that can be made of it, and redress for persons affected by data that is improperly sought or accessed.

EU Data retention legislation

e-Privacy Directive

Directive 2002/58/EC,[12] commonly known as 'the e-Privacy Directive', was adopted by the EU in July 2002. The e-Privacy Directive deals with aspects of privacy in telecommunications that are not covered by the EU's Data Protection Directive.[13] Among other matters, the e-Privacy Directive restricts how telecommunications service providers may retain and process 'traffic data' and 'location data' relating to their customers' use of their service. In general terms, it requires that these be retained for the minimum time necessary for billing and similar purposes. Unless the subscriber expressly consents otherwise, that data should be anonymised or erased when no longer required.

However, Article 15 creates an important exception to this general rule: Member States may legislate for the retention of subscribers' location or traffic data to safeguard against threats to national security, defence or public safety, or to combat crime and computer hacking. The Article requires any such measures to conform to what it refers to as "the general principles of Community law" and restricts them to those that are "necessary, appropriate and proportionate … within a democratic society".

[11] See, for example, the observations of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression quoted in the Murray Report at para. 35, pp. 17-19.
[12] Directive 2002/58/EC, available here.
[13] Directive 95/46/EC, available here. This directive will be replaced in May 2018 by the EU's General Data Protection Regulation, available here.

Data Retention Directive

In March 2006, the European Parliament and Council adopted the Data Retention Directive to harmonise Member States' data retention practices, to set standards for how communications data should be stored and to prescribe protections for individuals in relation to how and when state authorities might have access to their data.[14] Notably, the Data Retention Directive required Member States to ensure that telecommunications service providers collect all communications data generated by their subscribers and retain it for not less than six months and not more than two years. During the retention period, the data was to be accessible by authorities such as police and state security services, but only for strictly defined purposes (such as investigating serious crime or terrorism) and subject to conditions that respected individual's rights under EU law and international conventions, particularly the European Convention on Human Rights. The Data Retention Directive also obliged Member States to appoint a supervisory authority to ensure that service providers maintained the security of retained data to the standards mandated by the Data Protection and e-Privacy Directives.

The Data Retention Directive set a deadline for implementation by Member States of 15 September 2007. It was implemented to varying degrees by Member States but was declared invalid by the Court of Justice of the European Union in the *Digital Rights Ireland* decision of April 2014,[15] which is discussed in greater detail below.

Data retention in Ireland

Communications (Retention of Data) Act 2011

The State implemented the Data Retention Directive by means of the *Communications (Retention of Data) Act 2011*.[16] That Act requires telecommunications service providers in the State to collect and retain all communications data, including subscribers' names and identification numbers, the location from which communications originated and the address to which they linked.

The data must be retained for two years, the maximum permitted by the Data Retention Directive. The supervisory authority appointed to oversee the

[14] Directive 2006/24/EC, available here.

[15] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung, Seitlinger, Tscholl and Others*: Joined Cases C-293/12 and C-594/12, judgment of the Grand Chamber of the CJEU available here.

[16] Text of the *Communications (Retention of Data) Act 2011* (as amended) available here. The 2011 Act repealed and replaced Part 7 of the *Criminal Justice (Terrorist Offences) Act 2005* (available here) which also provided for retention of communications data.

standards of security under which data was retained is the Data Protection Commissioner.

Section 6 of the 2011 Act allows senior personnel in the Gardaí, Defence Forces, Revenue Commissioners and the Competition and Consumer Protection Commission ('CCPC') to have retained data disclosed to them. A senior officer of those agencies may request the data if he or she is satisfied that the data is required to prevent, detect, investigate or prosecute (in line with the responsibilities of the agencies in question) serious crimes, threats to human life or the security of the State, or serious tax offences or competition law offences.

The 2011 Act makes no provision for independent screening of requests to access retained data or for their prior approval by a court or supervisory body. However, section 10 allows a person who believes that data relating to him or her have been improperly disclosed to complain to the Referee (an independent judge or lawyer appointed by the Taoiseach) using the complaints mechanism provided for in the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*.[17] Section 12 of the 2011 Act adopts the review procedure that operates under the 1993 Act, whereby a judge keeps "the operation of the [2011] Act under review" and ascertains whether the authorities whose officers may make requests for access to communications data are complying with the Act's provisions. The designated judge reports to the Taoiseach at least annually, and his or her report is laid before the Houses of the Oireachtas.[18]

Statutory Instrument No. 336 of 2008

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 implement the e-Privacy Directive. Regulation 6 exempts retention pursuant to the *Communications (Retention of Data) Act 2011* from the general obligation to delete subscribers' location and traffic data when no longer required.[19]

[17] *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* available here.

[18] See, by way of example, the report of the designated judge for 2016, available here.

[19] S.I. No. 336/2011 – *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011,* available here.

The Digital Rights Ireland decision

In April 2014 the Court of Justice of the European Union ('CJEU') ruled that the Data Retention Directive was invalid and therefore had no legal effect.[20] The decision arose from cases questioning the validity of the Directive that had been taken in Ireland by Digital Rights Ireland (a civil rights advocacy group concerned with issues relating to telecommunications and data processing) [21] and in Austria by the provincial government of Carinthia and a group of more than 11,000 citizens.

The CJEU based its decision on the rights to privacy and family life and to protection of personal data that are assured under Articles 7 and 8 of the EU's Charter of Fundamental Rights.[22] The CJEU accepted that concerns such as organised crime and terrorism raised issues of public concern that could justify some interference with those rights, but it ruled that the type and degree of interference must be strictly limited and – most importantly – proportionate to the threat involved. Further, any provision allowing such interference must have adequate safeguards against abuse and loss of data security as well as suitable remedies for cases where safeguards fail. The CJEU held that:

- the Directive's requirement that service providers retain all communications data, even of persons not suspected of involvement in serious crime, was disproportionate;
- the Directive failed to set objective criteria determining how and when national authorities could access and use retained data;
- the Directive failed to protect rights by means of procedural safeguards such as prior review by a court; and
- the Directive's failure to stipulate that communications data be retained in the EU undermined the requirement to protect personal data.

The State's data retention regime has continued to operate without modification under the *Communications (Retention of Data) Act 2011*, notwithstanding that the Data Retention Directive (the implementation of which was the express purpose of the 2011 Act) was declared invalid by the CJEU.

---

[20] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung, Seitlinger, Tscholl and Others*: Joined Cases C-293/12 and C-594/12, judgment of the Grand Chamber of the CJEU available here.

[21] Digital Rights Ireland website accessible here.

[22] Text of the Charter of Fundamental Rights available here. The Charter is a constitutional document of the EU that binds the EU and its institutions. It is closely aligned with the European Convention on Human Rights and is interpreted so as to be consistent with decisions of the European Court of Human Rights.

The *Tele2* decision

In December 2016, the CJEU ruled in a case known as *Tele2* that EU law prohibited general and indiscriminate retention of traffic and location data. Further, even where data retention regimes met EU norms of proportionality (that is, that the measures adopted in a particular case reflect the scale of the problem being addressed) and specificity (that is, the avoidance of overly broad legislation or administrative measures) the CJEU held that procedural safeguards such as prior review by an independent body such as a court were essential.[23]

This decision arose from two related cases referred to the CJEU. In one, a Swedish telecommunications service provider, citing the *Digital Rights Ireland* decision, had refused official demands that it implement the Swedish data retention law that had been enacted to transpose the Data Retention Directive. In the other, the UK Courts had been asked to rule that aspects of the UK's data retention laws were legally invalid in light of the invalidity of the Data Retention Directive. Both the Swedish and UK laws resembled Ireland's 2011 Act in that they provided for the general and indiscriminate retention of traffic and location data.

The CJEU's decision hinges on Article 15(1) of the e-Privacy Directive. As noted above, that Article allows Member States to legislate for data retention measures to combat crime and threats to public order or national security. However, the Article sets limits on the scope of these measures: the retention must be "for a limited period justified on the grounds laid down in [Article 15(1)]". Further the retention must be limited to what is "necessary, appropriate and proportionate … within a democratic society", and the measures must comply with general principles of EU law. The CJEU found that the Swedish and UK legislation that were the subject of the case fell within Article 15(1) and on that basis could be assessed to determine their compatibility with the criteria it laid down.

Having regard to Articles 7 (privacy) and 8 (protection of personal data) of the Charter of Fundamental Rights,[24] the CJEU said that national legislation permitting data retention was permissible only to prevent serious crime and could not be based on "the general and indiscriminate retention of all traffic and location data".

To be permissible, retention must be restricted to data relating to particular times and places relevant to the crime being investigated or prevented, or to the data of persons involved or otherwise objectively relevant to an investigation or related activity of the authorities. The Swedish and UK measures before the CJEU exceeded the limits of what was strictly necessary and for that reason breached the latitude allowed by Article 15(1).

---

[23] *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson*: Joined cases C-203/15 and C-698/15, judgment of the Grand Chamber available here.

[24] Text of the Charter of Fundamental Rights available here

The Murray Report

In January 2016, the Tánaiste and then Minister for Justice and Equality, Frances Fitzgerald TD, commissioned former Chief Justice John Murray to undertake a review of the State's data retention laws with respect to the communications data of journalists. This followed the CJEU's *Digital Rights Ireland* decision as well as a controversy that arose when members of An Garda Síochána and the Garda Síochána Ombudsman Commission questioned journalists about their sources for certain stories and in some cases obtained access to their communications data, potentially compromising the confidentiality of the sources.[25]

Justice Murray completed the report of his review in April 2016. It was published by the Minister for Justice and Equality, Charlie Flanagan TD on 3 October 2017 after review by the Attorney General.[26] At the same time, the Minister also published the General Scheme of the *Communications (Retention of Data) Bill 2017*, which is the subject of this briefing paper.[27]

Because the *Tele2* decision addressed the validity of data retention measures under Member State legislation (rather than, as in the *Digital Rights* Ireland case, the validity of EU laws), it was particularly significant for the review: the observations and findings of the CJEU feature prominently in the Murray Report's analysis of the law and best practice regarding data retention.

In light of the *Tele2* decision, Justice Murray added a postscript to his report in which he recommended that statutory bodies authorised to request retained data under the 2011 Act consider whether, as a matter of policy, they should continue to do so.

The Murray Report criticised many aspects of the *Communications (Retention of Data) Act 2011,* which underpins the State's current data retention regime. The "principal frailties" that it notes are:[28]

- a lack of independent vetting and authorisation of access requests made by statutory bodies;
- a lack of coherence ("legislative scatter") in the statutory rules governing the retention and disclosure of data;
- failure of the Act to set out clear objective criteria governing data retention and disclosure;
- absence of clear procedures and protocols to be followed by authorities given access to retained data;

---

[25] Dáil Éireann, Debates (27 January 2016), available here. See also "Around a dozen journalists quizzed by Gardaí over their sources", Irish Examiner (15 January 2016) available here.

[26] Murray Report available here.

[27] Text of the General Scheme available here.

[28] Murray Report, para. 256, p. 115.

- failure to provide for notification of persons whose data is disclosed or who are affected by disclosure;
- a lack of remedies for wrongful access to retained data; and
- failure to require retained data to be kept within the EU.

The Murray Report made a number of recommendations for reform of the law and practices relating to retention of data. Some of the more far-reaching recommendations are summarised below:

Journalists

Issues relating to journalists and their sources were central to the review's terms of reference and are examined in considerable depth in the Murray Report. The report recommends that applications to access retained data of journalist should be made "only to a judge of the High Court".

Access to a journalist's retained data should in principle be permitted only when the journalist is suspected of committing a serious crime or threatening State security. For that reason, retaining or accessing data in order to identify journalists' sources should be permitted only when there is "an overriding requirement in the public interest."

Journalists, like other persons, should also have the benefit of safeguards including notification (at a suitable time) that their data has been retained or accessed, and have a right to redress for wrongful retention or disclosure of their data.[29]

Independent monitoring authority

The Murray Report recommends that an independent authority should be resourced and have power to ensure that telecommunications service providers maintain proper standards and adopt suitable procedures to ensure the security of retained data.[30] In this regard, service providers should be obliged to file a compliance statement with the monitoring authority that outlines their security measures, and to update the details in it as required.[31]

[29] Murray Report, paras. 231-237, pp. 105-106.

[30] *Ibid.*, paras. 282-292, pp. 125-128. The Report suggests the Data Protection Commissioner could be considered for this role.

[31] *Ibid.*, paras. 292-293, p. 129.

Disclosure requests

Requests for disclosure of retained data should be evaluated in accordance with the principle of proportionality. This means that the statutory authority or officer making the request must consider the availability of other less intrusive actions, and limit the scope of the request to the minimum required. Further, the disclosure requested must be strictly necessary to achieve a specific statutory objective.[32]

Requests for disclosure should in all cases be subject to authorisation by a judge or independent authority. Where the request is to disclose a journalist's sources, a High Court judge should decide.[33] Disclosure requests should be grounded on a statutory declaration containing all relevant information. Where disclosure of a journalist's sources is involved, that should be expressly stated.[34]

The Report recommends that there should be sanctions for wrongful access to retained data. These should include criminal penalties if the wrongful access was committed intentionally or recklessly.[35]

Statutory authorities

The Murray Report proposes that only a limited number of designated officers in statutory authorities should have authority to request disclosure of retained data. These officers should receive suitable training, including in privacy and on the principle of proportionality.[36]

It also recommends that disclosure requests should specify the exact offence being investigated, the relevance of the request to the investigation, and should be based on reasonable grounds for belief that the disclosure is the least intrusive option, proportionate and of an extent reasonably required for a permitted purpose.[37]

Statutory authorities should report to the Minister annually on the performance of its functions, and the Minister should be required to publish those reports or a summary of them.[38]

---

[32] *Ibid.*, para. 302, p. 132.

[33] Murray Report, para. 303, p. 133.

[34] *Ibid.*, para. 304, p. 133.

[35] *Ibid.*, para. 308, 341, p. 133-134, 145

[36] *Ibid.*, para. 326, p. 141.

[37] *Ibid.*, para. 325, 327, pp. 140, 141-142.

[38] *Ibid.*, para. 330-331, p. 142.

Right to notification

Persons whose retained data is disclosed should be notified of that fact once doing so is unlikely to prejudice an investigation. Persons whose rights have been affected should have an appropriate judicial remedy.[39]

[39] Murray Report, paras. 236, 336, pp. 106, 144

Outline of the General Scheme

Table 1 below summarises the measures proposed in each Head of the General Scheme.

Table 1: Outline of the General Scheme of the Communications (Retention of Data) Bill 2017

Head	Deals with	Description
1	Interpretation	Defines key terms including: • subscriber data • traffic and location data • competition offence • Revenue offence • serious offence
2	Non-application of Act	Provides that the contents of communications (such as the voice element of mobile or fixed-network telephony, or text and images communicated through email or opening websites) are not subject to retention and access under the Act.
3	Obligation to Retain Subscriber Data	Obliges telecommunications service providers to retain information identifying their subscribers for 12 months. Includes transitional provisions relating to subscriber data retained under the 2011 Act.
4	Disclosure request for subscriber data	Allows a designated officer of one of the statutory agencies to have subscriber data disclosed to him or her. The designated officer must have reasonable grounds for believing that the subscriber data: • relates to a person involved in a serious offence within the remit of that officer's agency, • is likely to assist in preventing, detecting, investigating or prosecuting such an offence, or • (in the case the Gardaí) may help to prevent or mitigate a serious and immediate risk to a person's health or safety, locate a missing person, or to assist a coroner's enquiries.
5	Application for Ministerial order for the retention of traffic and location data	Provides for the heads of relevant statutory agencies (An Garda Síochána, GSOC, Revenue Commissioners and Competition and Consumer Protection Commission) to request the Minister to order that service providers retain traffic and location data. The data must relate to specified persons or belong to specified categories.
6	Ministerial order to retain traffic and location data	Authorises the Minister, pursuant to a request under Head 5, to order retention of traffic and location data for up to 12 months. The Minister may vary, revoke or renew an order. Before making an order, the Minister must be satisfied as to the grounds for making it and that

Head	Deals with	Description
		doing so is proportionate.
7	Obligation to retain traffic and location data	Requires service providers to retain data in accordance with a Ministerial order under Head 6.
8	Application for order to disclose traffic and location data	Provides for designated officers to apply to an authorising judge for an authorisation to have retained traffic and location data disclosed to them. The designated officer must have reasonable grounds for believing that the data: • relates to a person involved in a serious offence within the remit of that officer's agency, • is likely to assist in preventing, detecting, investigating or prosecuting such an offence, or • (in the case the Gardaí) may help to prevent or mitigate a serious and immediate risk to a person's health or safety, location of a missing person, or to assist a coroner's enquiries. The designated officer must be satisfied that the disclosure is the least intrusive means available, is proportionate and is of an appropriate scale.
9	Appointment of panel of judges / judicial authorisation of disclosure	Provides for the appointment of judges by the President of the District Court to act as authorising judges. Also sets out the procedures for issuing authorisations pursuant to applications under Head 8. The judge must be satisfied as to the grounds on which the application was made and may impose conditions on the authorisation.
10	Variation/revocation of authorisation	Provides for variation by an authorising judge of an authorisation upon application by a designated officer. Also provides for revocation of an authorisation that is no longer needed.
11	Approval of disclosure in cases of urgency	Allows a designated officer to apply to a superior officer for authorisation of disclosure of traffic and location data. The request may be made only if: • the data involved is likely to be destroyed or otherwise become unavailable, • there is a serious and immediate risk to an individual's health or safety, or • the security of the State is likely to be compromised. The superior officer and the designated officer must both be satisfied that, but for the urgency, the conditions for obtaining an authorisation would be met to the satisfaction of an authorising judge. The superior officer must present a written report of the authorisation to the head of his or her agency within 7 days.
12	Data security	Requires service providers to maintain all retained data securely. The standard of security is to be the same as that required under the 2011 Act. Data must be retained within the EU.
13	Destruction	Provides for the irrevocable destruction of all data

Head	Deals with	Description
	arrangements	retained under the Act. Destruction is required within a month of the end of the 12-month retention period or, if the data has been disclosed under an authorisation, a month after the date when the relevant investigation or proceedings are concluded.
14	Access to data	Prohibits service providers from accessing retained data unless required by law or normal operating duties.
15	Notification post facto	Provides for the notification of persons whose data have been the subject of a disclosure request or whose interests are materially affected by one. Also provides for regulations to cover situations where an authorisation was issued on foot of the disclosure request. The regulations may provide for the non-disclosure of the authorisation unless disclosure is consistent with the purposes of the authorisation, the protection of personal privacy, preventing serious crime etc.
16	Designated officers	Provides for the designation of senior officers of the statutory agencies. These are to have power to apply for disclosure of retained data as provided for in Heads 4, 8 and 11 and related functions under the General Scheme
17	Penalties	Provides for criminal penalties for service providers for failure to: • retain subscriber or traffic and location data as required, • disclose retained data when duly requested, or • maintain data securely.
18	Review by designated judge	Provides for the operation of the Act to be kept under review by a High Court judge. The provision adopts the review mechanism in the *Interception of Postal Packets and Communications Messages (Regulation) Act 1993*. The judge's reports (as well as a report indicating whether information has been redacted from it) are laid before the Oireachtas by the Taoiseach.
19	Retention of materials	Provides for the retention of authorisations and supporting documents. These are to be retained for 3 years or until the end of the relevant investigation or proceedings, whichever is later.
20	Restriction of disclosure of existence of orders, authorisations etc.	Provides that the heads of the statutory agencies are responsible for the secure storage of "information and documents to which this [Act] applies", and that only persons authorised to do so may have access to them. Also provides for regulations to restrict disclosure of the existence of orders for retention and authorisations of disclosure.
21	Reporting	Provides that each of the statutory agencies must report annually to its respective Minister on disclosed data. The reports must detail the numbers of requests made, the number of disclosures made and the average time between

Head	Deals with	Description
		the date when the service provider first processed it and the date on which disclosure was requested. The Ministers are required to lay the reports before the Oireachtas within 6 months of receiving them.
22	Complaints Procedure	Provides for a complaints procedure to be available to: • persons who believe they might have been the subject of an authorisation, or • a superior officer who makes a report under Head 11 (Approvals in cases of urgency) where he or she believes an investigation is in the interests of justice. The Head adopts the Referee mechanism under the *Interception of Postal Packets and Communications Messages (Regulation) Act 1993*.
23	Regulations	Provides for regulations to be made by Ministers responsible for the statutory agencies in respect of the matters prescribed in the Heads. Regulations must be laid before the Oireachtas and may be annulled by a resolution of either House.
24	Repeal	Provides for the repeal of the *Communications (Retention of Data) Act 2011.*
25	Short title and commencement	Provides for the short title and for commencement in whole or part or for different purposes.
26	Schedule	Lists offences defined as 'serious offences' for the purposes of Garda requests for disclosure.
Source: General Scheme and L&RS		

Key Issues

Journalists and their sources

Former Chief Justice Murray's review of the State's data retention laws was commissioned in response to a controversy concerning Gardaí requests to access retained communications data of journalists, allegedly to identify sources of leaked confidential materials.[40]

The Murray Report[41] stresses the importance of journalism, journalists and their sources in a democratic society. The Report quotes the European Court of Human Rights' description of the protection of journalists' sources as "one of the basic conditions for press freedom" and notes that disclosure of a source should be permissible only if "justified by an overriding requirement in the public interest".

The Report further notes the similarity of reasoning adopted by the Irish Courts in cases concerning journalists' sources, and stresses the importance of prior judicial approval of any surveillance of the media that could compromise sources.[42] Based on this, the Report recommends that, in addition to the protections afforded to individuals generally:

- applications to disclose journalists' retained data for the purpose of disclosing sources "should be made only to a judge of the High Court". The law should expressly provide that access must be justified by "an overriding requirement in the public interest",[43] and

- access to a journalist's retained communications data for any purpose – including to identify a source – should in principle be permitted "only when the journalist is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State." Access where the journalist is not the person suspected should be permitted only where objective evidence shows that "vital national interests such as public security are at stake".[44]

The General Scheme does not address either of these recommendations or otherwise make particular provision for journalists or their sources.

---

[40] Dáil Éireann, debates (27 January 2016), available here. See also "Around a dozen journalists quizzed by Gardaí over their sources", Irish Examiner (15 January 2016) available here.

[41] Report available here.

[42] See generally Murray Report paras. 214-230, pp. 96-105.

[43] Murray Report, paras. 231 & 234, p. 105.

[44] *Ibid.*, para. 232-233. p. 105.

Key issue 1: Journalists and their sources

The terms of reference for the Murray Report specifically referenced the effect of data retention laws on the work of journalists and the confidentiality of their sources. Consideration of these issues form a significant part of the Report, which makes a number of specific recommendations concerning journalists and issues raised by retention of and access to their communication data. However, the General Scheme makes no reference to journalists or their sources and does not address recommendations dealing specifically with them.

The Committee had to consider:

- whether particular provision should be made in the proposed Act for journalists and their sources; if so,
- whether the provisions should reflect the recommendations in the Murray Report or different measures; and
- how 'journalist' and related terms should be defined.

Statutory bodies and designated officers

The Murray Report makes a number of recommendations concerning statutory bodies and their designated officers that are summarised in paras 325-331 on pp. 140-142 of the Report. Most of these are reflected in the General Scheme, but several are not.

Key issue 2: Statutory bodies and designated officers

The Murray Report recommended a number of safeguarding measures that should apply to statutory bodies authorised to access retained data and their designated officers. Many, but not all, of those recommendations are reflected in the General Scheme.

The Committee had to consider whether:

- there should be an express limit on the number of designated officers in each statutory body (e.g. 3 designated officers in the CCPC);
- requests to access retained data should be made by way of statutory declaration or affidavit specifying the exact statutory offence or facts justifying the request; and
- legislation should require all personnel involved in requesting access to retained data to receive formal instruction on the importance of proportionality.

Independent monitoring authority

The standard of security under which personal data is kept is one of the issues that come under the general oversight responsibility of the Data Protection Commissioner under the Data Protection Acts 1988 and 2003.[45] The Murray Report noted that this included data retained under the 2011 Act. In pursuance of Article 9 of the Data Retention Directive, section 4(2) of the 2011 Act designates the Data Protection Commissioner the national supervisory authority for monitoring the security of retained data, though the Murray Report characterised the way in which this was done as "perfunctory and inadequate", as the Act did not set out any criteria for measuring security compliance.[46]

The Report stressed the importance of an objective standard of data security that service providers should be obliged to maintain in respect of retained data. However, it said, the importance of such standards in EU law also required "a robust form of monitoring and supervision of Service Providers by an independent authority with a clearly defined role and expressly associated powers and duties". Resources, including appropriate personnel, would be necessary for such an authority. It suggested the Data Protection Commissioner as a candidate for undertaking this responsibility.[47] The Report further proposes that service providers be required to complete an annual compliance statement in respect of their security standards. Notably, it also recommends that retained data be stored in Ireland "thus ensuring that it is secured and that access to it is limited in accordance with the relevant criteria and safeguards laid down in Irish law".

Head 12 of the Bill sets standards of security for retained data that service providers must assure. The standards to be met are phrased in the same terms as the current provisions in section 4 of the 2011 Act (which in turn mirrors Article 7 of the Data Retention Directive). However, the Heads make no provision for an authority to monitor security compliance as recommended by the Murray Report, nor do they require service providers to produce compliance statements.[48] Head 12(1)(d) proposes that the data be retained "within the EU" rather than, as recommended in the Report, only in Ireland.[49]

Key issue 3: Independent monitoring authority

The Murray Report recommends that service providers be obliged to keep retained data at an appropriate and objectively verifiable standard of security, and that an independent authority be appointed to monitor compliance with those standards.

[45] Text of *Data Protection Act 1988* (as amended) available here; text of *Data Protection (Amendment) Act 2003* available here.
[46] Murray Report, para. 283, p. 126
[47] Murray Report, paras. 282-292, pp. 125-128.
[48] *Ibid.*, para. 289, p. 128
[49] *Ibid.*, para. 414, p. 170

The Committee had to consider:

- whether the security standards mandated by Heads 12 are appropriate;
- whether retained data should be required to be kept in the State;
- whether an authority should be appointed to monitor compliance with security standards and, if so,
- the powers and resources required for the proper performance of that authority's functions.

Statutory cohesion and mutual assistance

The Murray Report stressed that laws affecting right to privacy should be clear, accessible and foreseeable. This protects individuals against arbitrariness in how authorities exercise legal powers. In relation to interception of communications (and, by inference, similar conduct such as data retention) the Report quotes the European Court of Human Rights to the effect that laws should be sufficiently clear to give citizens "adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[50]

An aspect of current data retention law that was criticised in the Murray Report was a lack of coherence and clarity – referred to as 'legislative scatter' – in provisions identifying which bodies should be allowed access to retained data, and the terms on which they might do so. The Report instanced the Garda Síochána Ombudsman Commission ('GSOC'), which is not named in the 2011 Act, as a body whose officers are entitled to request access to retained data. Instead, GSOC asserts authority to do so under section 98 of the *Garda Síochána Act, 2005*, which gives its officers the same investigatory powers, immunities and privileges as any other member of the Garda Síochána.[51] The Report criticises this reliance on provisions that are not expressly related to data retention and points out that GSOC's access to data would not be subject to review by the designated judge under section 12 of the 2011 Act. However, it should be noted that Heads 4(6), 8(6), 13(3) and 16(4) of the General Scheme address these criticisms and expressly cover GSOC and how it may request and use retained data.

Another circumstance in which retained data is accessed but which is not expressly provided for in the 2011 Act is where a request is made by foreign authorities under section 75 of the *Criminal Justice (Mutual Assistance) Act,*

50 Murray Report, paras. 196-200, pp. 79-85

[51] Section 98 of the Garda Síochána Act 2005 (as amended) available here. The Murray Report expressed scepticism about aspects of GSOC's interpretation of this section: see Murray Report, para. 370-371, pp. 156-157.

2008.[52] That provision allows a member of An Garda Síochána not below the rank of inspector, on foot of a request from certain foreign police or security services, to request a judge of the District Court to authorise the disclosure of specified retained data. The Murray Report notes that the judge has no discretion to refuse an application made in the prescribed manner. It adds that there is no way to ascertain the number of requests of this type that have been made, but estimates it at approximately 250 per year "although the Review has been told that the annual number is steadily increasing."[53]

Key issue 4: Statutory cohesion and mutual assistance

The Murray Report criticises a lack of clarity in statutory provisions identifying which bodies may be given access to retained data, and the terms upon which they may be given such access.

The Committee had to consider:

- whether express provision should be made for access to retained data in circumstances not addressed in the General Scheme, such as where a request is made under the *Criminal Justice (Mutual Assistance) Act, 2008,* and
- whether safeguarding provisions of the General Scheme (such as Head 15 (notification of data requests), Head 18 (review by a dedicated judge), Head 21 (reporting) and Head 22 (complaints procedure)) should make provision for all cases where retained data is accessed, whether under the express terms of the General Scheme or otherwise.

Judicial remedy

The Murray Report notes the importance attached by the CJEU in the *Tele2* case to the availability of remedies for infringement of the rights affected by data retention: the CJEU cited Article 22 of the e-Privacy Directive, which requires Member States to "provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by national law applicable to [processing of data coming within the terms of the directive]" and Article 23 of the Data Protection Directive, which requires Member States to provide for compensation where a data subject suffers damage as a result of unlawful processing. The Murray Report describes the statutory remedies provided in Irish legislation in pursuance of those provisions[54] as inadequate to provide an appropriate remedy where fundamental rights have been infringed. It therefore

[52] Section 75 of the Criminal Justice (Mutual Assistance) Act 2008 (as amended) available here

[53] Murray Report, para. 125, p. 49

[54] Section 7 of the *Data Protection Act 1988*, available here; Regulation 16(2) of S.I. No. 336/2011 *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011*, available here

recommended that data retention legislation should "expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation."

Head 22 of the General Scheme provides for a complaint procedure for suspected breaches of the proposed Act. This is to be available to a person who believes that they might be the subject of an authorisation to retain traffic and location data or an authorisation to disclose it. It is also to be available to a superior officer who makes or receives a report of an approval issued in a case of urgency under Head 11 where that officer believes an investigation to be necessary in the interests of justice. The person may apply to the Referee established under section 9 of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*[55] to investigate whether an authorisation or approval was issued and, if it was, whether the conditions for granting it (or any conditions imposed in the authorisation or approval) were breached.

If the Referee determines that a breach occurred, he or she may:

- quash the authorisation or approval;
- order the destruction of the data and associated documentation; and
- report the matter to the head of the relevant statutory body and the designated judge who supervises the operation of the proposed Act.

If the Referee finds that no contravention occurred, he or she notifies the complainant of that fact. The Referee's decision is final.

Key issue 5: Judicial remedy

The Murray Report recommends that persons whose rights, potentially including fundamental rights, have been affected by wrongful access to retained data should have an appropriate judicial remedy. It notes that this is a principle supported by EU legislation and decisions of the European Court of Human Rights.

The General Scheme proposes a complaint procedure using the Referee mechanism under section 9 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993. Remedies available under this will include quashing of a wrongful authorisation or approval to access data, and destruction of that data. The Referee's decision is to be final.
The Committee may wish to consider whether this provides an appropriate remedy for cases where contravention of the proposed Act causes rights, potentially including fundamental rights, to be breached.

[55] Section 9 of the Interception of *Postal Packets and Telecommunications Messages (Regulation) Act, 1993* available here

Stakeholder views

The Committee held four stakeholder engagements over two weeks to discuss the provisions of the Bill. It first met with officials from the Department of Justice and Equality, who outlined the main aims of the Bill.

Department of Justice and Equality

Addressing the Joint Committee on the 8th of November 2017, officials of the Department of Justice and Equality explained that the purpose of the Bill is to update data retention law in Ireland in order to take account of evolving European Court of Justice jurisprudence in this area, particularly the *Digital Rights Ireland* and *Tele 2* judgments. The Department, in its submission, stated that:

> "While in strict legal terms the *Tele2 Sverige/Watson* judgement does not have direct effect in Irish law it sets down clear parameters on what Member States may provide for in national legislation in relation to data retention and as we are obliged to ensure that our law is in compliance with EU law, we have revised the original Heads of the Bill approved by Government in 2015 to also take account of the ruling in the Tele2 judgment."

The revised General Scheme is designed to respond to both EU Court of Justice rulings by:

- providing for Ministerial authorisation for the retention by service providers of targeted categories of traffic and location data for the purpose of the prevention, detection, investigation or prosecution of serious crime or safeguarding the security of the State;

- requiring judicial authorisation for disclosure of retained data to the Garda Síochána and other agencies;

- providing for notification of persons whose data have been disclosed when such notification is unlikely to jeopardise the investigation of an offence or to undermine the security of the State; and

- by providing for the data concerned to be held for a 12-month period and for that data to be held in the EU.

Overall oversight of the new legislation will continue to be vested in a High Court judge, with a judge of the Circuit Court independently investigating complaints.

In terms of implications for combating crime and protecting the security of the State, the Department added that the *Tele2 Sverige/Watson* judgement, which advocates the targeted retention of data based on objective evidence, is challenging from a law enforcement point of view. Thus, while the Bill takes account of the judgment and provides for the making by the Minister of orders for the retention of specified categories of data, the actual making of such orders will require careful consideration. No final decisions have been made on what specific categories of data might be the subject of Ministerial orders for targeted retention.

The Murray report and journalists' sources

The Department states that Mr Justice Murray's Review of the Law on the Retention of and Access to Communications Data was hugely helpful in preparing the General Scheme. The vast majority of its recommendations have been taken into account in the General Scheme, with a small number of issues to be resolved in finalising the Bill.

There are relatively few recommendations specific to accessing the data of journalists contained in the review, the key one of which is that access to journalists' retained data for the specific purpose of identifying their journalistic sources should be authorised by a judge of the High Court.

However, the approach advocated by the Minister is to apply the protection of judicial authorisation to every citizen in all cases, and not just to a particular class of citizen in particular cases. The revised Heads of the Bill propose that any application for authorisation to access any person's data (except in cases of urgency) must be approved by one of a number of designated District Court judges (this is the strictest form of compliance with the ruling of the European Court of Justice which requires authorisation either by a judge or an independent body). The hierarchy of a complaints procedure administered by a Circuit Court judge and oversight of operation of the Act by a High Court judge has been maintained.

Given the proposals in the Bill, the Minister's view is that making additional provisions for High Court authorisation for accessing journalists' data in certain cases could give rise to complexities. Such an authorisation would only apply in relation to requests for access to journalistic sources, so District Court authorisations would be required for all other access requests. The result would be that other categories of persons who may have sources, for example members of these Houses, would be treated differently. Search warrants, which are more intrusive in nature and which could result in actual content data being discovered, are issued by the District Court.

For these reasons, the Minister believes that there are strong arguments for a clear and consistent level of judicial protection for everyone's data. Questioned by Deputy Jack Chambers as to why the General Scheme had not followed the Murray report recommendations on including specific protections for journalistic sources, Ms Geraldine Moore replied that: "We did not think it would be appropriate that it would be appropriate to provide for particular categories of persons. We would have had to draw up a list of particular categories and we would end up with a two-tier regime. We have provided for the one data retention regime and all the protections apply to everyone equally."

Digital Rights Ireland

The Joint Committee also met with Digital Rights Ireland (DRI), which was represented by its Chairman, Mr TJ McIntyre, accompanied by Mr Simon McGarr, solicitor. The engagement took place on the 8th of November 2017.

In its submission, DRI was quite critical of the General Scheme, and questioned whether it would withstand future legal challenge. While welcoming the fact that some of the issues raised by Digital Rights Ireland in its constitutional challenge - commenced in 2005 - are finally being addressed by legislation, it believes the General Scheme still fails to meet the standards set by the European Court of Justice (CJEU) in its judgments in *Digital Rights Ireland* and *Tele2*. It identified the most important shortcomings as follows:

- The standard for making a Ministerial order to retain data is too permissive. It applies a test of proportionality while *Tele2* provides that data retention is only permissible in cases of strict necessity, i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary';

- There is no requirement that a Ministerial order to retain data must be targeted. *Tele2* requires that 'national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'. This requirement is not addressed in the General Scheme;

- The standard for access to data of third parties - those not involved in any wrongdoing - is too permissive. In relation to the investigation of crime, Tele2 requires that the person whose information is demanded must be in some way implicated in the crime: 'In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in

such a crime'. Heads 8 and 9 fail to impose this limitation and permit access to data of entirely unconnected third parties if 'likely to assist in the prevention, detection, investigation or prosecution of that offence'.

In light of these flaws, DRI believes, the General Scheme of the Bill does not meet the requirements of European Union Law.

Further, it believes the General Scheme has significant additional problems. For example:

- Head 22 seeks to abolish the current power of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation;

- Head 11 permits access to information about journalists' sources without judicial authorisation, in violation of Article 10 of the ECHR and contrary to the recommendations of the Murray Review;

- More generally, the General Scheme does not reform the structure for oversight of data retention, and continues to place too much reliance on a designated judge who acts on a part-time basis, with very limited transparency, and without the benefit of any technical or other expert support.

Observations on Individual Heads of Bill

Digital Rights Ireland offers the following observation and recommendations on individual Heads of the General Scheme:

Head 1: Definitions

The definition of 'traffic and location data' in this Head is exceptionally wide and could permit Ministerial orders to require ISPs to store information about what sites or individual web-pages were visited by individuals. By defining 'traffic and location data' to include any 'data processed for the purpose of sending, receiving or storing a communication by means of an electronic communications network' it could for example require an ISP to log URLs revealing the newspapers or even particular articles read by an individual. In this regard it would go significantly further than either the Data Retention Directive or the 2011 Act, neither of which imposed such a requirement, and would be even more problematic from a fundamental rights perspective.

DRI recommends that this definition be amended to make it clear that the Bill cannot be used to require the logging of information about web-browsing or other information which tends to reveal the content of communications. This could be done by redefining 'traffic and location data' to set out the precise

categories of data which can be retained, as was previously done in Schedule 2 of the Communications (Retention of Data) Act 2011.

Heads 5 and 6: Ministerial orders for data retention

a) The standard for making a Ministerial order to retain data in these Heads is too permissive. It creates a test of mere proportionality - using language such as 'likely to assist', 'proportionate', 'no alternative less intrusive means… likely to assist as effectively' – whereas *Tele2* provides that data retention is only permissible in cases of strict necessity, i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.

DRI recommends that Head 6 be modified to provide that an order shall not be made unless the retention of the data is strictly necessary as defined by the CJEU in *Tele2.*

b) *Tele2* requires that any national data retention rule must be 'targeted', which the CJEU defines in the following terms:

'the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected … [N]ational legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'.

Head 6 fails to include any provision to this effect, and instead gives a largely unfettered power to make rules requiring general data retention. As a result, it falls significantly short of the standards set out in *Tele2*. DRI recommends that it be amended to ensure that any data retention order be targeted as required by *Tele2*.

Head 7: Obligation to retain data

By providing a blanket data retention period of 12 months, rather than a tailored period which is 'strictly necessary' in the context of a particular data retention order, this Head fails to meet the requirement in *Tele2* that 'the retention period adopted [must be limited] to what is strictly necessary'.

DRI recommends that this Head be modified to provide that service providers must store the relevant data for the period specified by the Minister, and that Head 6 be modified to provide that a data retention order may be made for the minimum period strictly necessary, not exceeding 3 months in any event.

Heads 8 and 9: Application for authorisation to disclose traffic and location data

The standard for access to data of third parties - those not involved in any wrongdoing – is too permissive. In relation to the investigation of crime, *Tele2* creates a general rule that the person whose information is demanded must be in some way implicated in the crime. Heads 8 and 9 fail to impose this limitation and permit access to data of entirely unconnected third parties if there is a belief that the data is 'likely to assist in the prevention, detection, investigation or prosecution of that offence'.

DRI recommends that Heads 8(1), (5), (6) and (7) be narrowed to limit access to data, in the context of the investigation, etc. of crime, to persons 'implicated in a crime'.

Head 11: Urgency

a) This Head fails to provide for retrospective authorisation. The Murray Review recommended at para 390 that an urgency exception: 'should be provided for in national legislation, but should be accompanied by a requirement that the authority seeking disclosure must subsequently provide objective evidence of the need for urgent and immediate access without prior authorisation, and must submit, as soon as possible thereafter, an application to the independent body or designated judge for retrospective authorisation.'

DRI recommends that this Head be modified to require retrospective authorisation in such cases.

b) This Head permits journalists' sources to be identified without judicial authorisation. It also permits information identifying journalists' sources to be accessed in some cases without any judicial approval. In this it fails to meet the standards set out by the ECtHR in *Sanoma Uitgevers BV v. the Netherlands*, which requires that - even in cases of urgency - there must be a prior independent review by a judge or similar body before information capable of identifying sources is handed over or accessed.

DRI recommends that this Head be modified to prevent the urgency approval system being used in respect of information identifying journalists' sources.

Head 15: Notification post facto

The judgment in *Tele2* reflects an international trend towards notification after the fact of those who have been put under surveillance unless there is a compelling reason not to do so.

This Head, however, creates a range of exemptions from notification, including a vague catch-all at subhead (2)(a) where notification would not be 'consistent with the purposes for which the authorisation or approval concerned was issued or granted'. This open-ended provision is not consistent with the requirements of Tele2 that notification is required unless it is liable to jeopardise investigations - a formula which makes it clear that what is required is a concrete risk of harm.

Head 18: Designated Judge

This Head maintains the existing scheme of oversight by a designated judge of the High Court. DRI has a number of concerns about the limitations of this system:

In Ireland, a judge alone does not have sufficient resources and competence to exercise comprehensive control over state surveillance. Currently, a Designated Judge of the High Court reports annually to the Taoiseach on his examination of its operation. In addition, a Complaints Referee (normally a serving judge of the Circuit Court) is appointed to receive and investigate complaints from persons who believe that their communications have been unlawfully intercepted. The oversight role of the judiciary is 'ad hoc, after the fact, part-time function of a busy judge with no staff, specialist training or technical advisors'. It is at risk of 'over-reliance on the entities supposedly being monitored'. Indeed, a generalist judge operating alone cannot be expected to have the specialist knowledge necessary to assess surveillance systems without either training or technical advisors. As surveillance becomes more technically complex, judges increasingly lack the specialist knowledge needed to provide adequate oversight.

Data Protection Commissioner's role - carved out and underutilised

Currently, the Data Protection Commissioner (DPC) is also given a mandate to work with the Designated Judge and Complaints Referee in monitoring state surveillance activities. However, the ability to do so is undermined by the legislative carve-out regarding matters of state security, which provide that data protection law 'does not apply to… personal data that in the opinion of the Minister [for Justice] or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State'. This is coupled with specific exclusions elsewhere in the legislation. Consequently, while the DPC has examined surveillance in the criminal justice context – for example, a 2014 audit

of An Garda Siochana reviewed access to retained telecommunications data – this power does not extend to the state security context if the Executive objects to its use.

Further, while the 2011 Act permits the designated judge to communicate with the DPC in the exercise of his functions – presumably for assistance where necessary - as of July 2016 there was 'no record of the Designated Judge having ever contacted the Office of the Data Protection Commissioner as per section 12(4) since the inception of the Act'.

The carve out and underutilisation contradicts EU norms where data protection authorities are important sources of expertise and their involvement in the oversight system is crucial to its comprehensiveness and effectiveness. In seven EU member states, data protection authorities have powers over intelligence services that are equivalent to their powers over all other data controllers.

Parliamentary oversight

Ireland and Malta are the only two countries in the EU that do not provide for parliamentary oversight of intelligence activities. Parliamentary oversight is crucial precisely because of the secretive nature of security and intelligence activities. It counters the risk of regulatory capture of a solely judicial mechanism of accountability, whereby a small pool of judges hearing only from state agencies may come to lose their objectivity. The ability of oversight bodies to report directly to parliament (rather than solely to the executive) is a method to ensure intelligence services and oversight bodies are held accountable for their work.

DRI recommends that consideration should be given to the role of parliamentary oversight as part of a wider review of Irish surveillance practices generally (including interception of communications, use of surveillance devices and use of covert human intelligence sources).

Transparency and public reporting

Under the existing Irish system, the Complaints Referee has never produced a public report, so it is unclear how this role functions. A lack of transparency makes it impossible to determine its effectiveness in practice. The investigations and decisions of the Complaints Referee are not published and the Government has stated that it does not hold records on the number of complaints received or any details of such complaints. However, it appears that there has never been a successful complaint to the Complaints Referee in respect of either wrongful interception of communications or wrongful access to communications data.

In relation to the designated judge, annual reports have consisted exclusively of a few formulaic paragraphs which recite that on a particular day certain (unspecified) documents were inspected, certain (unspecified) queries answered and as a result the judge is satisfied that the relevant authorities are in compliance with the law. These reports provide no indication as to the methodology used (are random disclosure requests chosen and audited; are internal systems reviewed?), no indication of the circumstances in which these powers are being used, and no indication of the safeguards (if any) in place to prevent abuse or rectify errors.

The quality of reports from oversight bodies is crucial to transparency.

Technical competence/expertise

The role of designated judge is not required to have any special expertise in the area of surveillance and does not have any technical support. This is not in line with international standards. Oversight bodies should be able to rely on information and communication technology specialist to provide them with a better understanding of surveillance systems.

A number of EU countries explicitly require by law that oversight bodies have internal technical competence.

To date, the role of Designated Judge has been a part-time one, carried out over a single day or a few days each year. However, adequate protection requires more significant engagement.

Resources

The role of Designated Judge does not have any administrative support. However, adequate financial and human resources are required for effective oversight. The Irish system must also have adequate support to support oversight functions and to provide an institutional memory on the appointment of new judges to the role.

In light of the above, and as part of a wider reform of surveillance practices, DRI recommends that the Designated Judge be replaced by an independent supervisory authority. It should be accountable to parliament, chaired by a judge, and supported by a secretariat with sufficient technical expertise and financial resources to provide detailed support, including formalised public reports. This supervisory authority should also take on the oversight of interception of communications, use of surveillance devices, and use of covert human intelligence sources.

Head 22: Complaints procedure

a) Under the existing data retention regime the Complaints Referee has the power to order that compensation be paid to any person whose personal data was wrongfully disclosed. This Head quietly removes that power, without any justification, in a manner which appears to be designed to minimise the cost to the state of abuses by forcing complainants to use the more expensive court process instead. This failure to provide for compensation makes it more likely that the Irish oversight regime will be found inadequate in any subsequent challenge before the European Court of Human Rights.

DRI recommends that subhead (5) be modified to reinstate the power to award compensation provided for in the 2011 Act.

b) Under subhead (6), the Complaints Referee is restricted to issuing a formulaic notice in response to a complaint where they find that there has been no contravention. This enforced secrecy is essentially the same as the equivalent provision under the 2011 Act. Under that Act it served to ensure the secrecy of the fact that communications data had been disclosed. It does not, however, serve the same function under this Bill where there is no blanket secrecy and instead there is a presumption that individuals will be notified of the fact that their data has been disclosed. It does, however, hamper both the complainant and the Complaints Referee by preventing the giving of reasons or findings of fact in appropriate cases.

DRI recommends that this subhead be modified to provide that where the Complaints Referee concludes that there has not been a contravention then they may give such reasons for that decision as they consider appropriate, at least in those cases where a person has been notified of the fact of disclosure and therefore the same secrecy issues do not arise.

c) DRI recommends that this Head be modified to require the Complaints Referee to collate statistics as to the number of complaints made (and the number upheld) each year. This report should include details as to the number of complaints upheld and amount of compensation awards made in respect of each state agency.

Irish Council for Civil Liberties

The Committee held an engagement with the Irish Council for Civil Liberties (ICCL) on 15th November 2017. The ICCL was represented by Mr Liam Herrick, executive director; Ms Elizabeth Farries, information rights project manager; and Ms Maeve O'Rourke, senior research and policy analyst.

The ICCL and DRI outlined their views in a joint submission to the Committee. As such, the ICCL shares the view of DRI that the General Scheme of the Bill fails to meet the requirements of European Union (EU) Law set by European Court of Justice (CJEU) in its judgments in *Digital Rights Ireland* and *Tele2*; fails to adequately reflect European Convention of Human Rights (ECHR) norms; and fails to include key recommendations from the Murray Review of data retention.

The ICCL's recommendations, as outlined by Ms Farries, can be summarised as follows:

- **Explicit protection of journalist sources**: Per the Murray Review, expressly prohibit communications data access except in accordance with specific circumstances; allow prior authorisation only from a judge of the High Court or an independent judicial or administrative body; and permit data access only when a journalist - and not someone else - is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State.

- **Strict necessity**: Proportionality is insufficient. Per *Tele2*, a Ministerial Order for data retention should only be made where 'strictly necessary', i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.

- **Targeted Data Retention**: Per *Tele2*, a Ministerial Order for data retention must be targeted. There must be an established connection between the data to be retained and the objective pursued, including 'objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'.

- **Limited third party access:** Uphold the requirements of *Tele2* that the person whose information is demanded must be in some way implicated in the crime before access to their data can be granted.

- **Precise definitions of data:** Amend the definition of 'traffic and location data' to set out precise categories of data in order to preclude revealing

content, as Schedule 2 of the Communications (Retention of Data) Act 2011 did previously.

- **Notification:** Uphold the requirements of *Tele2* that those whose communications data is retained must be notified as soon as notification is not liable to jeopardise the investigations undertaken.

- **Judicial Remedy:** Per the Murray Review, 'bearing in mind the coercive character of a data retention system, and the concomitant risk to fundamental rights associated with it, that a statute should expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation'.

- **Institute an independent supervisory body:** In keeping with the trend of European Union member states, replace the Designated Judge with a unified independent supervisory agency. This agency should include parliamentary accountability, be chaired by a judge in a nearly full time position, and be supported by a secretariat with sufficient technical expertise and financial resources to provide detailed support including formalised public reports.

- **Limited retention period:** Uphold the requirements of *Tele2* that a Ministerial Order for Data Retention must be limited to what is strictly necessary and in any event no more than 3 months.

- **Urgent cases - mandate retrospective authorisation**: Uphold the recommendations of the Murray Review that urgency exceptions to disclosure authorisation requirements must require retrospective authorization in the form of objective evidence of a need for urgent and immediate disclosure.

- **Urgent cases - require a judge or oversight body:** Uphold the requirements of the *Sanoma* judgment that even urgent situations require independent review by a judge or similar body before information capable of identifying sources is handed over or accessed.

- **Compensation:** Retain the current power under the 2011 Act of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation.

- **Complaint notification reasons**: The Complaints Referee should notify the person who has applied for an investigation into data retention his or her reasoning in the event of a decision that there was no contravention of the Act.

- **Complaint reporting:** Require the Complaints Referee to collate statistics as to the number of complaints made, including details as to the number of complaints upheld and amount of compensation awards made in respect of each state agency.

National Union of Journalists

The Committee also met with the National Union of Journalists (NUJ), represented by Mr Seamus Dooley, at its engagement of November 15th 2017.

Noting that the Bill has profound implications for journalists and for media organisations, the NUJ believes that the highest level of protection, under both Irish Constitutional and international law, must be afforded to journalists in respect of privacy in their communications. The media plays a crucial role in maintaining accountability and transparency in the workings of civic society in a democratic state.

The NUJ believes that the General Scheme of the Communications (Data Retention) Bill 2017 does not make adequate provision for the protection of sources or afford the level of judicial oversight recommended by Mr Justice John Murray in his review of the legislative framework in respect of access by statutory bodies to communications data of journalists held by communications service providers.

The General Scheme, according to Mr Dooley, sets aside the key recommendations of Mr Justice Murray, and this is concerning. He urged the Committee to have due regard to the recommendations of Mr Justice Murray.

The NUJ welcomed the establishment of the Murray Review by the Tánaiste and Minister for Justice and Equality, announced on 19th January 2016. The Communications (Retention of Data) Act 2011 covers the retention and storage of historic data pertaining to all electronic communication, including fixed line and mobile telephone, internet communication and text messages and is being done without the consent of those affected. As Mr Justice Murray has pointed out, the arrangement is indiscriminate in application and scope, affecting the retention and storage of journalists' communications data pertaining to the time, date, location, destination and frequency of a journalist's telephone calls and can thus identify sources.

Location data linking a journalist's telephone calls with those of another caller before or after a sensitive meeting in which that person was known to have been involved can fatally compromise confidential sources of information, including from whistleblowers. The NUJ's approach to the protection of sources is firmly rooted not just in journalistic ethics but in international conventions.

The NUJ suggests that the Communications (Retention of Data) Bill 2017 should incorporate the recommendations on journalistic sources made by Mr Justice Murray. It is welcome that Mr Justice Murray recognises that the protection of journalistic sources is of vital importance to journalists in the exercise of their professional activities; and the NUJ highlighted in particular his recommendation that any exception which permits the identification of journalistic sources or which might oblige a journalist to disclose them should be subject to prior control by a judicial or independent administrative authority.

Mr Justice Murray recommends that applications must be made to a High Court Judge. It is of particular concern to the NUJ that Head 9 of the General Scheme makes provision for the designation of judges of the District Court for a panel to act as authorising judges: "In a sense, that decision is reflective of the low priority given under the General Scheme to the recommendation of Mr Justice Murray."

Mr Dooley contended that the current legislation in relation to the protection of sources is in conflict with the European Convention on Human Rights and demonstrably undermines the fundamental rights of journalists. The Minister has ignored the recommendation of the designation of a supervisory authority to ensure the legislation is not abused. This is also regrettable, he believes.

He concluded that the NUJ shares many of the concerns expressed by DRI and the ICCL. In particular, it shares the concern that the General Scheme does not reform the structure for oversight of data retention and does not comply with EU law. Head 22 seeks to abolish the current power of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation. There is urgent need for legislative reform in this area.

In relation to the issues of specific concern to the NUJ, it believes the report of Mr Justice Murray provides a framework for meaningful reform.

Recommendations

The Joint Committee is concerned to ensure that proposed data retention legislation is fully compliant with EU law and adequately reflects European Convention on Human Rights norms. As such, it makes the following recommendations:

1) *Journalists and their sources:* The Committee recommends that particular provision be made in the proposed Bill for journalists and their sources, and these provisions should reflect the recommendations of the report of Mr Justice Murray. Thus, applications to access retained data of a journalist should be made only to a judge of the High Court, or to an independent judicial or administrative body; retaining or accessing data in order to identify journalists' sources should be permitted only where there is "an overriding requirement in the public interest"; and access to a journalist's retained communications data for any purpose, including for the purpose of identifying his or her sources, should in principle be permitted only when the journalist (and not somebody else) is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State.

   It should be made explicit that retaining or accessing data in order to identity journalists' sources should be permitted only where prior judicial authorisation has been secured **and** there is an overriding requirement in the public interest.

2) *Rights to notification:* Persons whose retained data is disclosed should be notified of the fact once doing so is unlikely to prejudice an investigation.

   Where a person has applied for an investigation into the retention of his or her data, and the Complaints Referee concludes that there was no contravention of the legislation, the applicant should be notified of the reasons for that decision.

   The Complaints Referee should be required to compile data on the number of complaints made, the number of complaints upheld, and the amount of compensation awards made by each State agency.

3) *Judicial remedy:* The General Scheme proposes a complaint procedure that retains the Complaints Referee mechanism used under existing legislation. The Committee recommends, per the Murray Review, that persons whose rights, potentially including fundamental rights, have been affected by access to retained data should have an appropriate judicial remedy, expressly provided for in legislation.

4) *Independent monitoring authority:* The Committee believes that the current system, retained in the General Scheme, of oversight by a designated judge of the High Court, is not a sufficiently robust protection against the potential for excessive surveillance. A non-specialist judge will lack both the expertise and resources to provide adequate oversight as surveillance becomes increasingly technically complex.

   The Committee recommends therefore the establishment of an independent authority, chaired by a senior judge - to ensure compliance with appropriate data protection standards. This body should be fully accountable to the Houses of the Oireachtas and furnish periodic detailed reports on its activities; and it should be provided with the necessary resources and technical expertise to perform its functions.

5) *Test to be applied for retaining data:* The General Scheme applies a proportionality test in determining the standard for the making of a Ministerial order to retain data. However, this falls short of the stricter criteria established in the case law of the Court of Justice of the European Union. The Committee therefore recommends that a Ministerial Order for data retention should only be made where 'strictly necessary'. A time limit of no more than three months should also be set for the retention of such data.

6) *Targeted data retention:* The Committee believes that in order for the proposed legislation to be fully compliant with EU law, it must limit and clearly set out the circumstances in which data can be retained. In line with the *Tele2* judgment, a Ministerial Order for data retention must be targeted. There must be an established connection between the data to be retained and the objective pursued, including "objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security".

7) *Access to third party data:* Heads 8 and 9 of the General Scheme are overly permissive in permitting access to data of entirely unconnected third parties if "likely to assist in the prevention, detection, investigation or prosecution of that offence." This should be restricted, as per the *Tele2* ruling, so that a person whose information is demanded must be in some way implicated in the crime before access to his or her data can be granted.

8) *Precise definitions of data:* The definition of 'traffic and location data' in Head 1 of the General Scheme is potentially very broad in its scope. It should be amended to ensure that the legislation cannot be used to

require the logging of information about web browsing or other information which tends to reveal the content of communications. The precise categories of data that can be retained should be explicitly set out in the legislation.

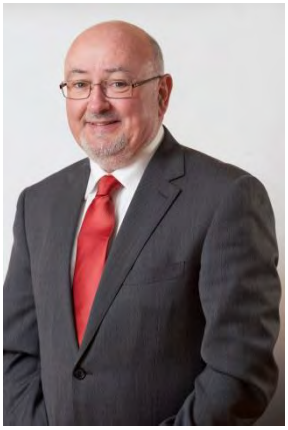
9) *Compensation:* The Committee believes that the current power under the 2011 Act of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation should be retained.

10) *Retrospective authorisation:* An urgency exception should only be provided for where accompanied by a requirement that the authority seeking disclosure must subsequently provide objective evidence of the need for urgent and immediate access without prior authorisation, and must submit, as soon as possible thereafter, an application to the independent body or designated judge for retrospective authorisation.

Appendix 1 – Committee Membership

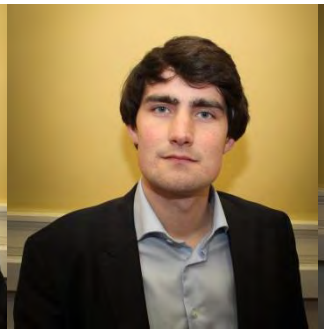
Joint Committee on Justice and Equality

Deputies

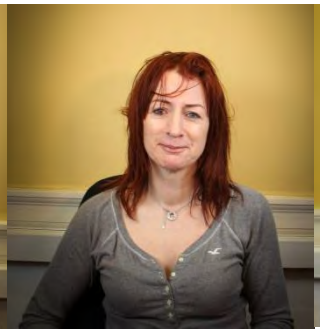


Caoimhghín Ó Caoláin TD
(SF) [Chair]

Colm Brophy TD
(FG)



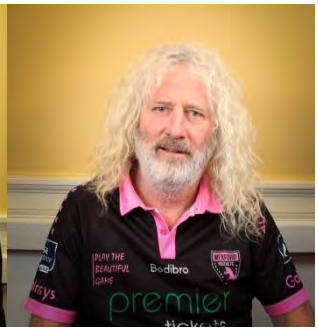
Jack Chambers TD
(FF)



Clare Daly TD
(I4C)

Alan Farrell TD
(FG)

Jim O'Callaghan TD
(FF)



Mick Wallace TD
(I4C)

Senators

Frances Black
(CEG)

Lorraine Clifford-Lee
(FF)

Martin Conway
(FG)

Niall Ó Donnghaile
(SF)

Notes:

1. Deputies nominated by the Dáil Committee of Selection and appointed by Order of the Dáil on 16th June 2016.
2. Senators nominated by the Seanad Committee of Selection and appointed by Order of the Seanad on 20th July 2016.

Appendix 2 – Terms of Reference of the Committee

JOINT COMMITTEE ON JUSTICE AND EQUALITY

TERMS OF REFERENCE

a. Functions of the Committee – derived from Standing Orders [DSO 84A; SSO 70A]

(1) The Select Committee shall consider and report to the Dáil on—

(*a*) such aspects of the expenditure, administration and policy of a Government Department or Departments and associated public bodies as the Committee may select, and

(*b*) European Union matters within the remit of the relevant Department or Departments.

(2) The Select Committee appointed pursuant to this Standing Order may be joined with a Select Committee appointed by Seanad Éireann for the purposes of the functions set out in this Standing Order, other than at paragraph (3), and to report thereon to both Houses of the Oireachtas.

(3) Without prejudice to the generality of paragraph (1), the Select Committee appointed pursuant to this Standing Order shall consider, in respect of the relevant Department or Departments, such—

(*a*) Bills,

(*b*) proposals contained in any motion, including any motion within the meaning of Standing Order 187,

(*c*) Estimates for Public Services, and

(*d*) other matters

as shall be referred to the Select Committee by the Dáil, and

(*e*) Annual Output Statements including performance, efficiency and effectiveness in the use of public monies, and

(*f*) such Value for Money and Policy Reviews as the Select Committee may select.

(4) The Joint Committee may consider the following matters in respect of the relevant Department or Departments and associated public bodies:

(*a*) matters of policy and governance for which the Minister is officially responsible,

(*b*) public affairs administered by the Department,

(*c*) policy issues arising from Value for Money and Policy Reviews conducted or commissioned by the Department,

(*d*) Government policy and governance in respect of bodies under the aegis of the Department,

(*e*) policy and governance issues concerning bodies which are partly or wholly funded by the State or which are established or appointed by a member of the Government or the Oireachtas,

(*f*) the general scheme or draft heads of any Bill,

(*g*) any post-enactment report laid before either House or both Houses by a member of the Government or Minister of State on any Bill enacted by the Houses of the Oireachtas,

(*h*) statutory instruments, including those laid or laid in draft before either House or both Houses and those made under the European Communities Acts 1972 to 2009,

(*i*) strategy statements laid before either or both Houses of the Oireachtas pursuant to the Public Service Management Act 1997,

(*j*) annual reports or annual reports and accounts, required by law, and laid before either or both Houses of the Oireachtas, of the Department or bodies referred to in subparagraphs (*d*) and (*e*) and the overall performance and operational results, statements of strategy and corporate plans of such bodies, and

(*k*) such other matters as may be referred to it by the Dáil from time to time.

(5) Without prejudice to the generality of paragraph (1), the Joint Committee appointed pursuant to this Standing Order shall consider, in respect of the relevant Department or Departments—

(*a*) EU draft legislative acts standing referred to the Select Committee under Standing Order 114, including the compliance of such acts with the principle of subsidiarity,

(*b*) other proposals for EU legislation and related policy issues, including programmes and guidelines prepared by the European

Commission as a basis of possible legislative action,

(*c*) non-legislative documents published by any EU institution in relation to EU policy matters, and

(*d*) matters listed for consideration on the agenda for meetings of the relevant EU Council of Ministers and the outcome of such meetings.

(6) Where a Select Committee appointed pursuant to this Standing Order has been joined with a Select Committee appointed by Seanad Éireann, the Chairman of the Dáil Select Committee shall also be the Chairman of the Joint Committee.

(7) The following may attend meetings of the Select or Joint Committee appointed pursuant to this Standing Order, for the purposes of the functions set out in paragraph (5) and may take part in proceedings without having a right to vote or to move motions and amendments:

(*a*) Members of the European Parliament elected from constituencies in Ireland, including Northern Ireland,

(*b*) Members of the Irish delegation to the Parliamentary Assembly of the Council of Europe, and

(*c*) at the invitation of the Committee, other Members of the European Parliament.

b. Scope and Context of Activities of Committees (as derived from Standing Orders) [DSO 84; SSO 70]

(1) The Joint Committee may only consider such matters, engage in such activities, exercise such powers and discharge such functions as are specifically authorised under its orders of reference and under Standing Orders; and

(2) Such matters, activities, powers and functions shall be relevant to, and shall arise only in the context of, the preparation of a report to the Dáil and/or Seanad.

(3) The Joint Committee shall not consider any matter which is being considered, or of which notice has been given of a proposal to consider, by the Committee of Public Accounts pursuant to Standing Order 186 and/or the Comptroller and Auditor General (Amendment) Act 1993; and

(4) any matter which is being considered, or of which notice has been given of a proposal to consider, by the Joint Committee on Public Petitions in the exercise of its functions under Standing Orders [DSO 111A and SSO 104A].

(5) The Joint Committee shall refrain from inquiring into in public session or publishing confidential information regarding any matter if so requested, for stated reasons given in writing, by—

(a) a member of the Government or a Minister of State, or

(b) the principal office-holder of a body under the aegis of a Department or which is partly or wholly funded by the State or established or appointed by a member of the Government or by the Oireachtas:

Provided that the Chairman may appeal any such request made to the Ceann Comhairle / Cathaoirleach whose decision shall be final.

(6) It shall be an instruction to all Select Committees to which Bills are referred that they shall ensure that not more than two Select Committees shall meet to consider a Bill on any given day, unless the Dáil, after due notice given by the Chairman of the Select Committee, waives this instruction on motion made by the Taoiseach pursuant to Dáil Standing Order 28. The Chairmen of Select Committees shall have responsibility for compliance with this instruction.

Appendix 3 – Witnesses and Official Report

8th November 2017:

- Officials from the Department of Justice and Equality; and
- Representatives from Digital Rights Ireland ('DRI').

Official report

15th November 2017:

- Representatives from the Irish Council for Civil Liberties; and
- Mr Seamus Dooley of the National Union of Journalists.

Official report

Irish Council for Civil Liberties

Digital Rights Ireland

Submission to Joint Committee on Justice and Equality
Communications (Retention of Data) Act Bill 2017
General Scheme Pre-Legislative Scrutiny
8 November 2017

Key Recommendations

Digital Rights Ireland (DRI) and the Irish Council for Civil Liberties (ICCL) thank the Committee for the opportunity to make submissions on the General Scheme of the Bill. We welcome the fact that some of the issues initially raised by Digital Rights Ireland in its constitutional challenge - commenced in 2005 - are being addressed by legislation.

That said, the General Scheme of the Bill fails to:

1. Meet the requirements of European Union (EU) Law set by European Court of Justice (CJEU) in its judgments in *Digital Rights Ireland* and *Tele2*;
2. Adequately reflect European Convention of Human Rights (ECHR) norms; and
3. Include key recommendations from the *Murray Review* of data retention.

We therefore recommend:

1. Explicit protection of journalist sources. Per the *Murray Review*, expressly prohibit communications data access except in accordance with specific circumstances; allow prior authorization only from a judge of the High Court or an independent judicial or administrative body; and permit data access only when a journalist - and not someone else - is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State.[1]

2. Strict Necessity. Proportionality is insufficient. Per *Tele2*, a Ministerial Order for data retention should only be made where 'strictly necessary', i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.[2]

3. Targeted Data Retention. Per *Tele2*, a Ministerial Order for data retention must be targeted. There must be an established connection between the data to be retained and the objective pursued, including 'objective evidence which makes it possible to identify a public whose data is

[1] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at paras 402 - 408.
[2] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.

likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'.[3]

4. Limited Third Party Access. Uphold the requirements of *Tele2* that the person whose information is demanded must be in some way implicated in the crime before access to their data can be granted.[4]

5. Precision Definitions of Data. Amend the definition of 'traffic and location data' to set out precise categories of data in order to preclude revealing content, as Schedule 2 of the Communications (Retention of Data) Act 2011 did previously.

6. Notification. Uphold the requirements of *Tele2* that those whose communications data is retained must be notified as soon as notification is not liable to jeopardise the investigations undertaken.[5]

7. Judicial Remedy. Per the *Murray Review*, 'bearing in mind the coercive character of a data retention system, and the concomitant risk to fundamental rights associated with it, that a statute should expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation'.[6]

8. Institute an Independent Supervisory Body. In keeping with the trend of European Union member states[7], replace the Designated Judge with a unified independent supervisory agency. This agency should include parliamentary accountability, be chaired by a judge in a nearly full time position, and be supported by a secretariat with sufficient technical expertise and financial resources to provide detailed support including formalised public reports.

We further recommend:

9. Limited Retention Period. Uphold the requirements of *Tele2* that a Ministerial Order for Data Retention must be limited to what is strictly necessary[8] and in any event no more than 3 months.

10. Urgent Cases - Mandate Retrospective Authorisation. Uphold the recommendations of *Murray Review* that urgency exceptions to disclosure authorization requirements must require retrospective authorization in the form of objective evidence of a need for urgent and immediate disclosure. [9]

11. Urgent Cases - Require a Judge or Oversight body. Uphold the requirements of *Sanoma* that even urgent situation require independent review by a judge or similar body before information capable of identifying sources is handed over or accessed. [10]

---

[3] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Paras.110-111.
[4] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.119.
[5] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.121.
[6] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 336.
[7] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017).
[8] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para. 108.
[9] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 390.
[10] *Sanoma Uitgevers BV v. the Netherlands*, application 38224/03, 14 September 2010.

12. Compensation. Retain the current power under the 2011 Act of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation.[11]

13. Complaint Notification Reasons. The Complaints Referee should notify the person who has applied for an investigation into data retention such reasons in the event of their decision that there was no contravention of the Act.

14. Complaint Reporting. Require the Complaints Referee to collate statistics as to the number of complaints made, including details as to the number of complaints upheld and amount of compensation awards made in respect of each state agency.

About us

Digital Rights Ireland

Digital Rights Ireland is a non-profit civil liberties group focusing on issues of technology and fundamental rights and has extensive experience in the area of privacy and data protection. DRI was the lead plaintiff in the judgment of the European Court of Justice in *Digital Rights Ireland and Seitlinger and Others* which invalidated the Data Retention Directive, and that action continues before the High Court in Dublin seeking to invalidate the Communications (Retention of Data) Act 2011 as well as earlier Irish data retention provisions. DRI was an *amicus curiae* in *Schrems*, which found the Safe Harbor decision on data transfers to the United States to be invalid, and was an *amicus curiae* in *Microsoft v. United States*, which prohibited extra-territorial access by the US Government to emails stored in Ireland.

Irish Council for Civil Liberties

The Irish Council for Civil Liberties is Ireland's leading independent human rights organisation. It monitors, educates and campaigns in order to secure full enjoyment of rights for everyone. Founded in 1976 by Mary Robinson and others, the ICCL has played a leading role in some of the most successful human rights campaigns in Ireland. These have included campaigns resulting in the establishment of an independent Garda Síochána Ombudsman Commission, the legalisation of the right to divorce, more effective protection of children's rights, the decriminalisation of homosexuality and introduction of enhanced equality legislation. The ICCL have previously given submissions to the 2016 commissioned review of *Communications (Retention of Data) Bill 2009*. They have also previously pursued privacy rights litigation with Liberty and others at the ECHR in relation to the UK's system of surveillance in the case of *Liberty and Others v The UK*, and *10 NGO and Others v The UK.*

TJ McIntyre **Chair** Digital Rights Ireland Company Limited by Guarantee contact@digitalrights.ie	Elizabeth Farries **Information Rights Project Manager** Irish Council for Civil Liberties International Network of Civil Liberties Organization elizabeth.farries@iccl.ie

[11] *Communications (Retention of Data) Act*, 2011, 3/2011.

Submission to Joint Committee on Justice and Equality
Communications (Retention of Data) Act Bill 2017
General Scheme Pre-legislative Scrutiny

8 November 2017

1. Summary

Digital Rights Ireland (DRI) and the Irish Council for Civil Liberties (ICCL) thank the Committee for the opportunity to make submissions on the General Scheme of the Bill. We welcome the fact that some of the issues raised by Digital Rights Ireland in its constitutional challenge - commenced in 2005 - are finally being addressed by legislation. That said, the General Scheme still fails to meet the standards set by the European Court of Justice (CJEU) in its judgments in *Digital Rights Ireland* and *Tele2*. Most importantly:

- The standard for making a Ministerial order to retain data is too permissive.[1] It applies a test of *proportionality* while *Tele2* provides that data retention is only permissible in cases of *strict necessity*, i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.[2]
- There is no requirement that a Ministerial order to retain data must be *targeted*. *Tele2* requires that 'national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'.[3] This requirement is not addressed in the General Scheme.
- The standard for *access to data of third parties* - those not involved in any wrongdoing - is too permissive. In relation to the investigation of crime, *Tele2* requires that the person whose information is demanded must be in some way implicated in the crime: 'In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime'.[4] Heads 8 and 9 fail to impose this limitation

[1] General Scheme Communications (Retention of Data) Bill 2017 at Head 6.
[2] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.
[3] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.111.
[4] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.119.

and permit access to data of entirely unconnected third parties if 'likely to assist in the prevention, detection, investigation or prosecution of that offence'.

In light of these flaws, the General Scheme of the Bill does not meet the requirements of European Union Law.

The General Scheme has significant further problems which we will address throughout these submissions. For example:

- Head 22 seeks to abolish the current power of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation.
- Head 11 permits access to information about journalists' sources without judicial authorisation, in violation of Article 10 of the ECHR and contrary to the recommendations of the Murray Review.

More generally, the General Scheme does not reform the *structure for oversight* of data retention, and continues to place too much reliance on a designated judge who acts on a part-time basis, with very limited transparency, and without the benefit of any technical or other expert support. We recommend that the institutional oversight for this (and other forms of surveillance) be revisited and make recommendations for reform.

Not only does the General Scheme fail to comply with EU law, but the General Scheme leaves a fragmented system of oversight in place that does not include key recommendations from the Murray Review of data retention and does not adequately reflect European Convention of Human Rights (ECHR) norms.

Our submissions should not be taken accepting that data retention as a principle is permissible or desirable. While we address the requirements needed to bring the General Scheme in line with EU law and ECHR norms, the requirements of domestic constitutional law have yet to be determined. It may be that the ongoing DRI litigation before the High Court will set more stringent standards under Bunreacht na hEireann. These submissions should therefore not be taken as conceding that the domestic standards are the same as the international standards. In this area, the EU/ECHR standards are a floor rather than a ceiling.

2. The Judgments in *Digital Rights Ireland* and *Tele2*

Following the 2016 revelation that the Garda Siochana Ombudsman Commission was accessing journalists' communication records from Service Providers under the aegis of the *Communications (Retention of Data) Act*, *2011* (2011 Act)[5], the Minister for Justice and Equality commissioned an independent review of communications data legislation. Former Chief Justice Mr. John L. Murray headed the Review (the Murray Review)[6] and gave recommendations for amending legislation.

[5] Communications (Retention of Data) Act, 2011, 3/2011.
[6] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017).

The Murray Review recommendations are based in large part on EU and ECHR Law. They refer in particular to two key judgments by the CJEU. The first is the judgment in *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources & Others* (*Digital Rights Ireland*).[7] That case was referred by the Irish High Court to the CJEU, which resulted in the invalidation of the EU Data Retention Directive (the Directive)[8]. The second is the subsequent CJEU judgment in *Tele2 Sverige AB v Post-Och Telestyrelsen* (*Tele2*)[9] which, building on *Digital Rights Ireland*, sets out binding standards which must be met to make any national system of data retention permissible under EU law and in particular the EU Charter of Fundamental Rights.

3. Key Principles

To protect the privacy rights of people living in Ireland under Article 8 ECHR, and their freedom of expression under Article 10 ECHR, it is crucial that the General Scheme explicitly addresses, at a minimum, the following key principles of EU/ECHR law as identified in the Murray Review:

Protection of journalist's sources

Data retention poses a particular threat to the Article 10 ECHR guarantee of freedom of expression, including a free media, which the European Court of Human Rights (ECtHR) has described as a structural support for democratic governance.[10] The Murray Review noted that 'the protection of journalistic sources is one of the basic conditions for press freedom… without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest'.[11]

The Murray Review therefore recommended that amending legislation governing access to retained communications data should:

- Expressly prohibit access for the purpose of identifying a journalist's sources except in accordance with the circumstances and conditions laid down in that legislation;
- Require prior authorisation to access journalists' information from a judge of the High Court (i.e. no authorisation at the level of the District Court and no emergency authorisations within agencies); and

[7] *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources & Others* (Joined cases C-293/12 and C-594/12).
[8] Directive 2006/24/EC 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
[9] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15.
[10] *Goodwin v United Kingdom* 1996 EHRR 123, cited in Murray, J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 218.
[11] Adopted by the Committee of Ministers of the Council of Europe on 8th March, 2000, Appendix, cited in Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 61.

- Be permitted only when the journalist - and not someone else - is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State.[12]

The General Scheme fails to implement these recommendations and fails to provide any higher standards for actions aimed at identifying journalists' sources. We recommend that it be modified to implement these recommendations.

Grounds for interference with privacy: strict necessity and direct nexus

Under the Irish Constitution[13] and numerous European and international human rights instruments,[14] the permissibility of interferences with the right to respect for privacy depends on their necessity and proportionality.

a) Strict necessity

In *Tele2* the CJEU identified that data retention is, in effect, a form of pre-emptive surveillance and therefore set out a higher standard of *strict necessity* before data retention can be required.[15] Mere utility or even proportionality is not sufficient. Necessity does not mean that legislation can permit data retention simply because it would be useful to investigatory bodies. As the Advocate General explained in his Opinion in *Tele2*, 'given the requirement of strict necessity, it is imperative that national courts do not simply verify the mere utility of general data retention obligations, but rigorously verify that no other measure or combination of measures, such as the targeted data retention obligation accompanied by other investigatory tools, can be as effective in the fight against serious crime'.[16] Heads 5 and 6 fail to meet this standard by providing for Ministerial data retention orders to be made on a weaker standard than strict necessity. We recommend that they be modified to refer to strict necessity.

b) Direct nexus

To meet the standards set out in *Tele2*, the law must demonstrate a direct nexus between the person whose information is demanded and the crime. The CJEU in *Tele2* noted that 'access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious

[12] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at paras 402 - 408.

[13] The Irish Constitution protects the right to privacy as an unenumerated right under Article 40.3, as established in the 1987 case of Kennedy v Ireland, [1987] IR 587.

[14] Universal Declaration of Human Rights, Article 12; International Covenant on Civil and Political Rights, Article 17; and regional standards including the Charter on Fundamental Rights of the European Union (2000/C 364/01) and the European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8. See also Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation , Article 17; see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

[15] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at paras. 96, 107 - 110

[16] Cited in Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para 209.

crime or of being implicated in one way or another in such a crime.'[17] As discussed further under Heads 8 and 9, the General Scheme fails to require such a nexus. We recommend that these be modified to do so.

4. Observations on Individual Heads of Bill

Head 1: Definitions

The definition of 'traffic and location data' in this Head is exceptionally wide and could permit Ministerial orders to require ISPs to store information about what sites or individual web-pages were visited by individuals. By defining 'traffic and location data' to include any 'data processed for the purpose of sending, receiving or storing a communication by means of an electronic communications network' it could for example require an ISP to log URLs revealing the newspapers (e.g. http://www.independent.ie) or even particular articles (e.g. http://irishcatholic.com/articulating-catholic-ethos/) read by an individual.

In this regard it would go significantly further than either the Data Retention Directive or the 2011 Act, neither of which imposed such a requirement, and would be even more problematic from a fundamental rights perspective.

This loose definition is not cured by Head 3, which states that the Bill 'does not apply to the content of communications' – a URL is not in and of itself content, notwithstanding that it will often reveal the content of a webpage.

We recommend that this definition be amended to make it clear that the Bill cannot be used to require the logging of information about web-browsing or other information which tends to reveal the content of communications. This could be done by redefining 'traffic and location data' to set out the precise categories of data which can be retained, as was previously done in Schedule 2 of the Communications (Retention of Data) Act 2011.

Heads 5 and 6: Ministerial orders for data retention

a) Standard is not that of strict necessity

The standard for making a Ministerial order to retain data in these Heads is too permissive. The test is set out in Head 6 as follows:

> '(3) The Minister shall not make an order under subsection (1) unless he or she is satisfied that the retention of the data to which the order relates –
> (a) is likely to assist in the prevention, detection, investigation or prosecution of serious offences or the safeguarding of the security of the State, and
> (b) is in all the circumstances proportionate;

[17] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at para. 119

> and that there are no alternative less intrusive means which would be likely to assist as effectively in the prevention, detection, investigation or prosecution of serious offences, or in the safeguarding of the security of the State.'

This creates a test of *mere proportionality* - using language such as 'likely to assist', 'proportionate', 'no alternative less intrusive means… likely to assist as effectively' - while *Tele2* provides that data retention is only permissible in cases of *strict necessity*, i.e. where 'the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.[18]

We recommend that Head 6 be modified to provide that an order shall not be made unless the retention of the data is strictly necessary as defined by the CJEU in *Tele2.*

b) No requirement that data retention be targeted

Tele2 requires that any national data retention rule must be 'targeted', which the CJEU defines in the following terms:

> 'the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected… [N]ational legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'.[19]

Head 6 fails to include any provision to this effect and instead gives a largely unfettered power to make rules requiring general data retention. As a result it falls significantly short of the standards set out in *Tele2.* We recommend that it be amended to ensure that any data retention order be targeted as required by *Tele2*.

Head 7: Obligation to retain data

By providing a blanket data retention period of 12 months, rather than a tailored period which is 'strictly necessary' in the context of a particular data retention order, this Head fails to meet the requirement in *Tele2* that 'the retention period adopted [must be limited] to what is strictly necessary'.

We recommend that this Head be modified to provide that service providers must store the relevant data for the period specified by the Minister, and that Head 6 be modified to provide that a data retention order may be made for the minimum period strictly necessary, not exceeding 3 months in any event.

---

[18] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.
[19] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Paras.110-111.

Heads 8 and 9: Application for authorisation to disclose traffic and location data

The standard for *access to data of third parties* - those not involved in any wrongdoing - is too permissive. In relation to the investigation of crime, *Tele2* creates a general rule that the person whose information is demanded must be in some way implicated in the crime: 'In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime'.[20]

Heads 8 and 9 fail to impose this limitation and permit access to data of entirely unconnected third parties if there is a belief that the data is 'likely to assist in the prevention, detection, investigation or prosecution of that offence'. For example, Head 8(1) provides that Gardai may apply for traffic and location data where they:

> '[H]ave reasonable grounds for believing that [the data] while not directly related to a person who is suspected of being or having been involved in the commission of the offence, are nevertheless likely to assist in the prevention, detection, investigation or prosecution of that offence.'

We recommend that Heads 8(1), (5), (6) and (7) be narrowed to limit access to data, in the context of the investigation, etc. of crime, to persons 'implicated in a crime'.

Head 11: Urgency

a) Fails to provide for retrospective authorisation

The Murray Review recommended at para 390 that an urgency exception: 'should be provided for in national legislation, but should be accompanied by a requirement that the authority seeking disclosure must subsequently provide objective evidence of the need for urgent and immediate access without prior authorisation, and must submit, as soon as possible thereafter, an application to the independent body or designated judge for retrospective authorisation.'

This Head fails to address this recommendation. We recommend that it be modified to require retrospective authorisation in such cases.

b) Permits journalist's sources to be identified without judicial authorisation

Head 11 also permits information identifying journalists' sources to be accessed in some cases without any judicial approval. In this it fails to meet the standards set out by the ECtHR in *Sanoma Uitgevers BV v. the Netherlands*[21] which requires that - even in cases of urgency - there must be a prior independent review by a judge or similar body before information capable of identifying sources is handed over or accessed. In that case the ECtHR stated that:

[20] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.119.
[21] *Sanoma Uitgevers BV v. the Netherlands*, application 38224/03, 14 September 2010.

> 'First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. The principle that in cases concerning protection of journalistic sources 'the full picture should be before the court' was highlighted in one of the earliest cases of this nature to be considered by the Convention bodies (British Broadcasting Corporation, quoted above (see paragraph 54 above)). The requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not.
>
> The Court is well aware that it may be impracticable for the prosecuting authorities to state elaborate reasons for urgent orders or requests. In such situations an independent review carried out at the very least prior to the access and use of obtained materials should be sufficient to determine whether any issue of confidentiality arises, and if so, whether in the particular circumstances of the case the public interest invoked by the investigating or prosecuting authorities outweighs the general public interest of source protection. It is clear, in the Court's view, that the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality.'[22]

We recommend that this Head be modified to prevent the urgency approval system being used in respect of information identifying journalists' sources.

Head 15: Notification post facto

The judgment in *Tele2* reflects an international trend towards notification after the fact of those who have been put under surveillance unless there is a compelling reason not to do so. The standard is articulated at para 121 which provides that:

> 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, *inter alia*, their right to a legal remedy... where their rights have been infringed.'

This Head, however, falls short of this standard in subhead (2). That subhead creates a range of exemptions from notification, including a vague catch-all at subhead (2)(a) where notification would not be 'consistent with the purposes for which the authorisation or approval concerned was issued or granted'. This open-ended provision is not consistent with the requirements of *Tele2* that notification is required unless it is liable to jeopardise

[22] *Sanoma Uitgevers BV v. the Netherlands*, application 38224/03, 14 September 2010,paras. 91-92.

investigations - a formula which makes it clear that what is required is a concrete risk of harm.

Head 18: Designated Judge

This Head maintains the existing scheme of oversight by a designated judge of the High Court. We discuss the limitations of this system in section 5 below.

Head 22: Complaints procedure

a) Removal of power to order compensation

Under the existing data retention regime the Complaints Referee has the power to order that compensation be paid to any person whose personal data was wrongfully disclosed.[23] This Head quietly removes that power, without any justification, in a manner which appears to be designed to minimise the cost to the state of abuses by forcing complainants to use the more expensive court process instead. This failure to provide for compensation makes it more likely that the Irish oversight regime will be found inadequate in any subsequent challenge before the European Court of Human Rights.

We recommend that subhead (5) be modified to reinstate the power to award compensation provided for in the 2011 Act.

b) Restriction on decisions of Complaints Referee

Under subhead (6), the Complaints Referee is restricted to issuing a formulaic notice in response to a complaint where they find that there has been no contravention. This enforced secrecy is essentially the same as the equivalent provision under the 2011 Act. Under that Act it served to ensure the secrecy of the fact that communications data had been disclosed. It does not, however, serve the same function under this Bill where there is no blanket secrecy and instead there is a presumption that individuals will be notified of the fact that their data has been disclosed. It does, however, hamper both the complainant and the Complaints Referee by preventing the giving of reasons or findings of fact in appropriate cases.

We recommend that this subhead be modified to provide that where the Complaints Referee concludes that there has not been a contravention then they may give such reasons for that decision as they consider appropriate, at least in those cases where a person has been notified of the fact of disclosure and therefore the same secrecy issues do not arise.

c) Statistics and reporting

We recommend that this Head be modified to require the Complaints Referee to collate statistics as to the number of complaints made (and the number upheld) each year. This

[23] Communications (Retention of Data) Act 2011, Section 10(5) (b).

report should include details as to the number of complaints upheld and amount of compensation awards made in respect of each state agency.

5. Institutional Oversight

The CJEU has through a series of judgments held that independent and effective supervision by a DPA is an essential component of the right to personal data protection, particularly in the context of surveillance.[24] The UN Office of the High Commissioner for Human Rights (OHCHR) has concluded similarly that 'an independent civilian oversight agency, is essential to ensure the effective protection of the law'.[25] In a comprehensive 2017 report on the EU fundamental rights framework regarding state surveillance, the European Union Agency for Fundamental Rights (EU FRA) stated that independence should not only be enshrined in law but adequately applied in practice'.[26] Enshrined monitoring practices by independent bodies like DPAs are also recognised to contribute to the development and improvement of internal safeguards in intelligence services.[27] While organised in diverse ways, there are many EU examples, with 16 of the 28 member states including expert bodies overseeing intelligence services.[28]

Under both the 2011 Act and the General Scheme, we note the following significant concerns:

Judge alone insufficient

In Ireland, a judge alone does not have sufficient resources and competence to exercise comprehensive control over state surveillance. Currently, a Designated Judge of the High Court reports annually to the Taoiseach on his examination of its operation. In addition, a Complaints Referee (normally a serving judge of the Circuit Court)[29] is appointed to receive and investigate complaints from persons who believe that their communications have been unlawfully intercepted. The oversight role of the judiciary is 'ad hoc, after the fact, part-time function of a busy judge with no staff, specialist training or technical advisors'.[30] It is at risk

[24] Cited in European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), see in particular CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014, para. 68; CJEU, C-362/14, *Maximillan Schrems v. Data Protection Commissioner*, 6 October 2015, para. 41 adn 66. See also Working Group on Data Protection in Telecommunications (2017).

[25] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in a Digital Age*, June 30, 2014, 12–13, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[26] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11.

[27] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p56.

[28] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p68.

[29] Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, Section 9.

[30] Privacy International and Digital Rights Ireland, *The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland* (September 2015) at para 28.

of 'over-reliance on the entities supposedly being monitored'.[31] Indeed, a generalist judge operating alone cannot be expected to have the specialist knowledge necessary to assess surveillance systems without either training or technical advisors. As surveillance becomes more technically complex, judges increasingly lack the specialist knowledge needed to provide adequate oversight.[32]

Data Protection Commissioner's role - carved out and underutilised

Currently, the Data Protection Commissioner (DPC) is also given a mandate to work with the Designated Judge and Complaints Referee in monitoring state surveillance activities. However, the ability to do so is undermined by the legislative carve-out regarding matters of state security, which provide that data protection law 'does not apply to… personal data that in the opinion of the Minister [for Justice] or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State'.[33] This is coupled with specific exclusions elsewhere in the legislation.[34] Consequently, while the DPC has examined surveillance in the criminal justice context – for example, a 2014 audit of the Garda Síochána reviewed access to retained telecommunications data[35] – this power does not extend to the state security context if the Executive objects to its use.

Further, while the 2011 Act permits the designated judge to communicate with the DPC in the exercise of his functions – presumably for assistance where necessary - as of July 2016 there was 'no record of the Designated Judge having ever contacted the Office of the Data Protection Commissioner as per section 12(4) since the inception of the Act'.[36]

The carve out and underutilisation contradicts EU norms where data protection authorities are important sources of expertise and their involvement in the oversight system is crucial to its comprehensiveness and effectiveness. In seven EU member states, data protection

[31] Privacy International and Digital Rights Ireland, *The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland*, (September 2015) at paras. 28 - 30. 'This has been highlighted by two recent examples of abuse: a 2010 case in which a Garda sergeant was found to be using the data retention system to spy on her former partner; and in 2014 when the Data Protection Commissioner (DPC) published an audit into the handling of information in the Garda Síochána it identified a number of problems in relation to data retention, all of which the Designated Judge had failed to identify.'.

[32] For example, in the US the President's Review Group and the Privacy and Civil Liberties Oversight Board have examined the operation of the FISC and in both cases have concluded that it needs additional technical guidance to carry out its work effectively. See President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (Washington, DC, 2013), chapter VI; Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Washington, DC, January 23, 2014), pt. 8, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[33] The Data Protection Acts 1988 and 2003, Section 1(4).

[34] For example, any restrictions on the processing of personal data 'do not apply if the processing is… in the opinion of a member of the Garda Síochána [of a certain rank] or an officer of the Permanent Defence Force [of a certain rank] and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the security of the State'. (The Data Protection Acts 1988 and 2003, Section 8.)

[35] Data Protection Commissioner, 'An Garda Síochána: Final Report of Audit,' March 2014, 61, available at: http://www.garda.ie/Documents/User/An%20Garda%20S%C3%ADoch%C3%A1na%20ODPC%20Report%20Final.pdf.

[36] Email of 18 July 2016 from the Office of the DPC in connection with EU Fundamental Rights Agency report into surveillance oversight. On file with TJ McIntyre.

authorities have powers over intelligence services that are equivalent to their powers over all other data controllers.[37]

Parliamentary oversight

Ireland and Malta are the only two countries in the EU that do not provide for parliamentary oversight of intelligence activities.[38] European and international human rights bodies have explained that effective oversight of state surveillance activities requires the involvement not just of the judiciary and executive (as provided for under the General Scheme), but *also* of parliament. In a comprehensive report, the EU Fundamental Rights Agency recommended that a full range of actors including parliament must be involved in holding intelligence services accountable.[39] The UN Office of the High Commissioner for Human Rights (OHCHR) has also concluded that 'the involvement of all branches of government in the oversight of surveillance programmes...is essential to ensure the effective protection of the law'.[40]

Parliamentary oversight is crucial precisely because of the secretive nature of security and intelligence activities.[41] It counters the risk of regulatory capture of a solely judicial mechanism of accountability, whereby a small pool of judges hearing only from state agencies may come to lose their objectivity.[42] The ability of oversight bodies to report directly to parliament (rather than solely to the executive) is a method to ensure intelligence services and oversight bodies are held accountable for their work.

We recommend that consideration should be given to the role of parliamentary oversight as part of a wider review of Irish surveillance practices generally (including interception of communications, use of surveillance devices and use of covert human intelligence sources).

Transparency and public reporting

Under the existing Irish system, the Complaints Referee has never produced a public report, so it is unclear how this role functions. A lack of transparency makes it impossible to determine its effectiveness in practice. The investigations and decisions of the Complaints Referee are not published and the Government has stated that it does not hold records on

[37] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p56.
[38] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p66.
[39] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights , Safeguards and Remedies in the EU: Volume II: Field Perspectives and Legal Update* (Luxembourg, 2017) p65
[40] Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in a Digital Age,' June 30, 2014, 12–13, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
[41] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), citing Born H and Leigh I, *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies* (Parliament of Norway Publishing House, Oslo, 2005) 16.
[42] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p56

the number of complaints received or any details of such complaints.[43] However, it appears that there has never been a successful complaint to the Complaints Referee in respect of either wrongful interception of communications or wrongful access to communications data.[44]

In relation to the designated judge, annual reports have consisted exclusively of a few formulaic paragraphs which recite that on a particular day certain (unspecified) documents were inspected, certain (unspecified) queries answered and as a result the judge is satisfied that the relevant authorities are in compliance with the law.[45] These reports provide no indication as to the methodology used (are random disclosure requests chosen and audited; are internal systems reviewed?), no indication of the circumstances in which these powers are being used, and no indication of the safeguards (if any) in place to prevent abuse or rectify errors.

The quality of reports from oversight bodies is crucial to transparency. The EU FRA recommends that:

> 'EU Member States should ensure that oversight bodies' mandates include public reporting to enhance transparency. The oversight bodies' reports should be in the public domain and contain detailed overviews of the oversight systems and related activities (e.g. authorisations of surveillance measures, on-going control measures, *ex-post* investigations and complaints handling).'[46]

Technical competence/expertise

The role of designated judge is not required to have any special expertise in the area of surveillance and does not have any technical support. This is not in line with international standards. The EU FRA's October 2017 report states that 'EU Member States should grant oversight bodies diverse and technically-qualified professionals'.[47] The ECHR also held in *Klass v Germany* that supervisory mechanisms must be 'vested with sufficient competence to exercise and effective and continuous control'[48] over state surveillance activities. Oversight bodies should be able to rely on information and communication technology specialist to provide them with a better understanding of surveillance systems.

---

[43] Dan MacGuill, *State Surveillance: How Gardaí and Others Can Secretly Monitor You,* TheJournal.ie (May 2015) Available at: http://www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai-2099537-May2015/.

[44] Dan MacGuill, *State Surveillance: How Gardaí and Others Can Secretly Monitor You*, TheJournal.ie, (May 2015) Available at: http://www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai- 2099537-May2015/; Dáil Debates, Written Answers, 4 March 2008, 122-123. http://debates.oireachtas.ie/dail/2008/03/04/unrevised2.pdf.

[45] The Right to Privacy in Ireland Stakeholder Report Universal Periodic Review 25th Session – Ireland at para 26.

[46] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p12.

[47] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11.

[48] *Klass v Germany*, Application no 5029/71 (ECtHR, 6 September 1978) para 56

A number of EU countries explicitly require by law that oversight bodies have internal technical competence.[49] A number of EU expert bodies also recruit external technicians, either on an *ad hoc* or more permanent basis.[50]

Part time basis

To date, the role of Designated Judge has been a part-time one, carried out over a single day or a few days each year. However, adequate protection requires more significant engagement. The Council of Europe Commissioner for Human Rights has noted that 'in contrast to parliamentary oversight committees, expert bodies conduct their work on a (near) full time basis. This generally means they can provide more comprehensive and in-depth scrutiny that their parliamentary counterparts'[51]

Resources

The role of designated judge does not have any administrative support. However, adequate financial and human resources are required for effective oversight. The EU FRA's October 2017 report states that 'EU Member States should grant oversight bodies adequate financial and human resources'.[52] The Irish system must also have adequate support to support oversight functions and to provide an institutional memory on the appointment of new judges to the role.

In light of the above, and as part of a wider reform of surveillance of surveillance practices we recommend that the designated judge be replaced by an independent supervisory authority, with parliamentary accountability, to be chaired by a judge, and supported by a secretariat with sufficient technical expertise and financial resources to provide detailed support including formalised public reports. This supervisory authority should also take on the oversight of interception of communications, use of surveillance devices, and use of covert human intelligence sources.

6. About us

Digital Rights Ireland

Digital Rights Ireland is a non-profit civil liberties group focusing on issues of technology and fundamental rights and has extensive experience in the area of privacy and data protection. DRI was the lead plaintiff in the judgment of the European Court of Justice in *Digital Rights Ireland and Seitlinger and Others* which invalidated the Data Retention Directive, and that action continues before the High Court in Dublin seeking to invalidate the Communications

[49] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p12.
[50] A number of EU expert bodies also recruit external technicians, either on an *ad hoc* or more permanent basis (2015), p84
[51] Council of Europe Commissioner for Human Rights (2015), p. 47 - cited in FRA October 2015 report at 43.
[52] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11

(Retention of Data) Act 2011 as well as earlier Irish data retention provisions. DRI was an *amicus curiae* in *Schrems*, which found the Safe Harbor decision on data transfers to the United States to be invalid, and was an *amicus curiae* in *Microsoft v. United States*, which prohibited extra-territorial access by the US Government to emails stored in Ireland.

Irish Council for Civil Liberties

The Irish Council for Civil Liberties is Ireland's leading independent human rights organisation. It monitors, educates and campaigns in order to secure full enjoyment of rights for everyone. Founded in 1976 by Mary Robinson and others, the ICCL has played a leading role in some of the most successful human rights campaigns in Ireland. These have included campaigns resulting in the establishment of an independent Garda Síochána Ombudsman Commission, the legalisation of the right to divorce, more effective protection of children‟s rights, the decriminalisation of homosexuality and introduction of enhanced equality legislation. The ICCL have previously given submissions to the 2016 commissioned review of *Communications (Retention of Data) Bill 2009*. They have also previously pursued privacy rights litigation with Liberty and others at the European Court of Human Rights in relation to the UK Ministry of Defence's system of surveillance in the case of *Liberty and others v The United Kingdom*.

Dr. TJ McIntyre Chair Digital Rights Ireland, CLG Castle Hill, Bennettsbridge Road, Kilkenny contact@digitalrights.ie	Elizabeth Farries Information Rights Project Manager Irish Council for Civil Liberties International Network of Civil Liberties Organization 9-13 Blackhall Place Dublin 7 +353-1-799 4504 elizabeth.farries@iccl.ie

Department of Justice and Equality

Joint Committee on Justice and Equality

Pre-legislative scrutiny of the

General Scheme of the Communications (Data Retention) Bill 2017

Opening Statement

I would like to thank the Chairman and the Joint Committee for this opportunity to participate in the pre-legislative scrutiny of the General Scheme of the Communications (Retention of Data) Bill which was published in October last.

The purpose of the Bill is to update data retention law in Ireland in order to take account of evolving European Court of Justice jurisprudence in this area.

By way of background to the General Scheme, the Communications (Retention of Data) Act 2011 provides the legal basis for the retention and subsequent disclosure of both telephone and internet data for the purpose of the prevention, detection, investigation and prosecution of serious offences and safeguarding the security of the State. The data in question is subscriber data (the identity of the subscriber) and traffic and location data (such as the location of a mobile phone and the numbers of other mobile phones it has communicated with). Access to such data is very important in the context of both combating serious crime and safeguarding the security of the State.

In its judgement of April 2014 in the *Digital Rights Ireland* case, the European Court of Justice found the EU Data Retention Directive to be incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The judgement was the consequence of the referral of a number of questions, concerning the compliance of the EU Data Retention Directive with the EU Charter of Fundamental Rights, to the Court of Justice by the Irish High Court.

In particular, the Court found that –

- the Directive went beyond what is necessary in that by requiring subscriber, traffic and location data to be held by service providers, it entailed an interference with the lives of almost all citizens in Europe and not just those linked to serious crime;

- the Directive did not expressly provide that access to and subsequent use of the data should be restricted to the purpose of preventing serious offences;

- the Directive did not provide for prior review by a court or by an independent administrative body when law enforcement agencies sought access to meta data;

- there was no clear basis in the Directive for the length of time that service providers were obliged to retain the data.

In light of the ruling, the Government approved the drafting of a revised Communications (Retention of Data) Bill which would take cognisance of the findings of the Court.

However, in December 2016, the Court of Justice considered the issue of data retention again and in its ruling in *Tele2 Sverige/Watson* (which related to data retention law in Sweden and the UK) the Court adopted a strict interpretation of its previous ruling in *Digital Rights Ireland*. The Court found:

- that national legislation providing for general and indiscriminate retention of traffic and location data for the purpose of fighting crime was in breach of the Charter of Fundamental Rights – it did not, however, preclude Member States from adopting legislation permitting the targeted retention of such data,

- that EU law precluded national legislation from providing for data retention and disclosure which was not restricted to fighting serious crime, where access was not subject to prior review by a court or independent administrative authority and where there was no legal requirement for the data concerned to be retained within the European Union.

Existing legislation

The 2011 Act already provides for a number of the requirements identified by the Court. The current Act provides that data can only be accessed by specific agencies where the data is required for the prevention, detection, investigation or prosecution of a serious offence, the safeguarding of the security of the State or the saving of human life.

Additional safeguards provided for in the legislation to protect the data in question include data security provisions, data destruction provisions and restriction on access to retained data. The legislation also provides for oversight of its operation by a High Court Judge who reports to the Taoiseach at least annually (with discretion to report more frequently) and for a complaints referee (a Circuit Court judge) to deal with the concerns of any person who believes that their data may have been unlawfully accessed in breach of the Act. These safeguards have been retained in the revised Bill.

However, the existing legislation requires service providers to retain internet data for one year and telephone and mobile data for two years and allows the Garda Síochána and other State agencies to make direct requests to service providers for retained data for investigative purposes and, as such, the legislation needs to reflect those elements of the Court of Justice rulings.

Revision of Heads of Bill

While in strict legal terms the *Tele2 Sverige/Watson* judgement does not have direct effect in Irish law it sets down clear parameters on what Member States may provide for in national legislation in relation to data retention and as we are obliged to ensure that our law is in compliance with EU law, we have revised the original Heads of the Bill approved by Government in 2015 to also take account of the ruling in the Tele2 judgment.

The revised General Scheme which you have before you responds to both EU Court of Justice rulings –

- by providing for Ministerial authorisation for the retention by service providers of targeted categories of traffic and location data for the purpose of the prevention, detection, investigation or prosecution of serious crime or safeguarding the security of the State;

- by requiring judicial authorisation for disclosure of retained data to the Garda Síochána and other agencies;

- by providing for notification of persons whose data have been disclosed when such notification is unlikely to jeopardise the

investigation of an offence or to undermine the security of the State, and

- by providing for the data concerned to be held for a 12 month period and for that data to be held in the EU.

Overall oversight of the new legislation will continue to be vested in a High Court Judge with a Judge of the Circuit Court independently investigating complaints.

Implications for combating crime and protecting the security of the State

It has to be said that the *Tele2 Sverige/Watson* judgement, which advocates the targeted retention of data based on objective evidence, is challenging from a law enforcement point of view. While the Bill takes account of the judgment and provides for the making by the Minister of orders for the retention of specified categories of data, the actual making of such orders will require careful consideration.

No final decisions have been made on what specific categories of data might be the subject of Ministerial orders for targeted retention.

The Murray report

In January 2016, following reports alleging inappropriate access of telephone records of certain journalists, the Government commissioned a review of the law in this area. In his Review of the Law on the Retention of and Access to Communications Data, Mr. Justice Murray took account of the *Tele 2 Sverige/Watson* judgement. Most of the review is taken up with an analysis of the 2011 Data Retention Act with recommendations on how the Act might be amended in light of the judgement. This report has been hugely helpful to us in preparing these proposals. The vast majority of its recommendations have been taken into account in the General Scheme, with a small number of issues to be resolved in finalising the Bill.

There are relatively few recommendations specific to accessing the data of journalists contained in the review, the key one of which is that access to journalists' retained data for the specific purpose of identifying their journalistic sources should be authorised by a judge of the High Court.

The approach advocated by the Minister is to apply the protection of judicial authorisation to every citizen in all cases and not just to a particular class of citizen in particular cases. The revised Heads of the Bill propose that any application for authorisation to access any person's data (except in cases of urgency) must be approved by one of a number of designated District Court judges (this is the strictest form of compliance with the ruling of the European Court of Justice which requires authorisation either by a judge or an independent body). The hierarchy of a complaints procedure administered by a Circuit Court judge and oversight of operation of the Act by a High Court judge has been maintained.

Given the proposals in the Bill, making additional provisions for High Court authorisation for accessing journalists' data in certain cases could give rise to complexities. Such an authorisation would only apply in relation to requests for access to journalistic sources, so District Court authorisations would be required for all other access requests. The result would be that other categories of persons who may have sources, for example members of these Houses, would be treated differently. Search warrants, which are more intrusive in nature and which could result in actual content data being discovered, are issued by the District Court.

For these reasons, the Minister believes that there are strong arguments for a clear and consistent level of judicial protection for everyone's data, but of course he would welcome the Committee's views.

The Minister forwarded a copy of Justice Murray's review together with the revised Heads of the Bill so that the Committee could examine the proposed legislation and the review together in considering the Minister's proposal for a balanced and proportionate data retention regime providing a high level of protection for all citizens.

Main Provisions of the General Scheme

You will have read through the Heads of the Bill. The key new provisions are -

Heads 3 and 4 (Obligation to retain subscriber data) / (Disclosure request for subscriber data) which place an obligation on service providers to retain subscriber data for a period of 12 months from the date on which the data were first processed and allow the competent authorities to make direct requests to service providers for that data.

Heads 5 and 6 (Application for Ministerial order for the retention of traffic and location data) / **(Ministerial order to retain traffic and location data)** which provide for applications to be made by the competent authorities for Ministerial orders for the targeted retention of categories of traffic and location data or traffic and location data in respect of specified persons for the purpose of the prevention, detection, investigation or prosecution of serious crime or safeguarding the security of the State and for the making of Ministerial orders to retain such data.

Head 8 (Application for authorisation to disclose traffic and location data) which allows a competent authority to apply to an authorising judge for an authorisation to make a disclosure request.

Head 15 (Notification post facto) which provides for the notification of a person who has been the subject of a disclosure request or other persons whose interests have been materially affected by the disclosure request.

Most of the other provisions of the Bill relating to data security, data destruction arrangements, restrictions on access to retained data, the complaints procedure and oversight of the operation of the Act by a High Court judge have been taken from the existing 2011 Act.

Submission to the Joint Committee on Justice and Equality

General Scheme of the Communications (Data Retention) Bill 2017

November 2017

Opening statement by Séamus Dooley, Irish Secretary, National Union of Journalists, (UK & Ireland) to the Joint Committee on Justice and Equality, Wednesday 15th November 2017

Chairman, Members of the Committee,
On behalf of the National Union of Journalists (NUJ) I am grateful for the opportunity to address the committee as part of the pre-legislative scrutiny of the General Scheme of the Communications (Data Retention) Bill 2017.

This Bill has profound implications for journalists and for media organisations.

The NUJ believes that the highest level of protection, under both Irish Constitutional and international law, must be afforded to journalists in respect of privacy in their communications. The media plays a crucial role in maintaining accountability and transparency in the workings of civic society in a democratic state.

Where the rights of the media are undermined the ability of journalists to shine a light into the darkest corners are severely curtailed.

While there is an individual right of privacy afforded to citizens, the right of privacy afforded to journalists in the exercise of their professional function is rooted in a public good that extends beyond the individual rights of citizens.

The General Scheme of the Communications (Data Retention) Bill 2017 does not make adequate provision for the protection of sources or afford the level of judicial oversight recommended by Mr Justice John Murray in his review of the legislative framework in respect to access by statutory bodies to communications data of journalists held by communications service providers.

Mr Justice Murray was asked to take into account "the principle of protection of journalistic sources; the need for statutory bodies with investigative/and or prosecution powers to have access to data in order to prevent and detect serious crime; and current best international practice in this area".

The Committee will be aware that Mr Justice Murray found that current data-retention legislation amounts to mass surveillance of the entire population of the State and recommended a series of changes to the current statutory framework, which he found was in breach of European law.

The General Scheme before the committee this morning sets aside the key recommendations of Mr Justice Murray and this is as concerning as it is curious.

In scrutinising the proposed legislative I respectfully suggest that the committee have due regard to the recommendations of Mr Justice Murray.

Mr Chairman, the NUJ welcomed the establishment of the Murray Review by the Tánaiste and Minister for Justice and Equality announced on 19th January 2016.

In establishing the review the Minister announced that it was anticipated that the review would be completed in three months. On October 19th 2016 Minister Fitzgerald advised the NUJ that the report was at “an advanced stage”.

The report was presented by Mr Justice Murray in April 2017 but only published on October 3rd 2017.

The fact that the Minister for Justice and Equality published the Murray Review and the General Scheme of the Communications (Data Retention) Bill 2017 simultaneously is an acknowledgement that the two are interlinked and my comments today are predicated on our submission to Mr Justice Murray.

The events leading to the establishment of the review provided a context to our submission.
The NUJ was gravely concerned at revelations in January, 2016 that the Garda Services Ombudsman Commission had authorised its investigators to demand access to the mobile ‘phone records of two journalists, on foot of its powers under section 98 of the Garda Síochána Act, exercised in the context of a disclosure request for telephone records made under section 6 of the Communications (Retention of Data) Act, 2011.

We met the Minister for Justice and Equality and with GSOC and raised our concerns with both.
In the case of GSOC we have a robust but respectful exchange of views on general principles.

The Communications (Retention of Data) Act 2011 covers the retention and storage of historic data pertaining to all electronic communication, including fixed line and mobile telephone, internet communication and text messages and is being done without the consent of those affected.

As Mr Justice Murray has pointed out, the arrangement is indiscriminate in application and scope, affecting the retention and storage of journalists’ communications data pertaining to the time, date, location, destination and frequency of a journalist’s telephone calls and can thus identify sources.

Location data linking a journalist’s telephone calls with those of another caller before or after a sensitive meeting in which that person was known to have been involved can fatally compromise confidential sources of information, including from whistleblowers and it was in this context that the NUJ expressed particular concern at the actions of GSOC.

The Minister subsequently announced the Ministerial Review and at this stage we would like to acknowledge the forensic work undertaken by Mr Justice Murray.

The NUJ’s approach to the protection of sources is firmly rooted not just in journalistic ethics but in international conventions.

Our submission to the Murray Review is attached as Appendix A, since it sets out the context for our approach to the General Scheme of the Communications (Data Retention) Bill 2017.

It is worth noting that Head 18 makes provision for a High Court judge to keep the operations of the provisions of the Bill under review.

Committee members will perhaps understand a degree of scepticism on our part against the backdrop of the decision not to incorporate key recommendations of the former Chief Justice into the new legislation.

The NUJ suggests that the Communications (Retention of Data) Bill 2017 should incorporate the recommendations on journalistic sources made by Mr Justice Murray.

For ease of references these are:
231. Applications by a statutory body for authorization to access a journalist's retained communications data for the specific purpose of determining his journalistic sources should be made only to a judge of the High Court. (R)
232. Access to a journalist's retained communications data for any purpose, including for the purpose of identifying his or her sources, should in principle be permitted only when the journalist is the object of investigation for suspected commission of a serious criminal offence or for unlawful activity which poses a serious threat to the security of the State. (R)
233. Accordingly, contrary to what is permitted under the 2011 Act it should not be permissible to access a journalist's retained data for the purpose of investigating an offence committed by someone else. This limitation should be subject only to 'particular situations' (referred to at paragraph 119 of the Tele2 Judgment) where vital national interests such as public security are at stake and there is objective evidence justifying access. (R)
234. In addition, as regards any statutory regime for the retention of communications data, express provision should be made by law prohibiting access by State authorities to retained data for the purpose of discovering a journalist's sources unless such access is fully justified by an overriding requirement in the public interest. (R)
235. A journalist whose retained communications data has been accessed should, as in the case of any other person similarly affected, be notified of that fact as soon as such 106 notification would no longer be likely to prejudice any investigation or prosecution of a serious criminal offence. (R)
236. The general recommendation that express provision be made for judicial remedies in the case of unlawful access of a person's retained communications data should, ipso facto, be available to journalists who considers their rights have been infringed by any such access. (R)
237. As already pointed out, in addition to these particular safeguards, access to a journalist's retained communications data for any purpose will also benefit from the full range of safeguards recommended in respect of such access generally by State authorities.

It is welcome that Mr Justice Murray recognises that the protection of journalistic sources is of vital importance to journalists in the exercise of their professional activities and the attention of the committee is drawn, in particular, to his recommendation:
223: Any exception which permits the identification of journalistic sources or which might oblige a journalist to disclose them should be subject to prior control by a judicial or independent administrative authority.

Mr Justice Murray recommends (231) that applications must be made to a High Court Judge.

It is of particular concern that Head 9 of the General Scheme makes provision for the designation of judges of the District Court for a panel to act as authorising judges.

In a sense that decision is reflective of the low priority given under the General Scheme to the recommendation of Mr Justice Murray.

I note that in publishing the General Scheme the current Minister for Justice and Equality acknowledged that while there are problems with the current legislation he emphasised that it was not unconstitutional.

The current legislation in relation to the protection of sources is in conflict with the ECHR and demonstrably undermines the fundamental rights of journalists.

I note that the Minister has ignored the recommendation of the designation of a supervisory authority to ensure the legislation is not abused. This is also regrettable.

Chairman, Members of the Committee, we share many of the concerns expressed by Digital Rights Ireland and the ICCL.

In particular, we share the concern that the General Scheme does not reform the structure for oversight of Data Retention and does not comply with EU law.

Head 22 seeks to abolish the current power of the Complaints Referee to award compensation to individuals whose data has been accessed in contravention of the legislation.

There is urgent need for legislative reform in this area. In relation to the issues of specific concern to the National Union of Journalists we believe the report of Mr Justice Murray provides a framework for meaningful reform.

Séamus Dooley
Irish Secretary
National Union of Journalists
November 2017

APPENDIX A

Independent Review of the Law in Respect of Access to the Communications Data of Journalists

"We need to constantly remind ourselves of the commitments we have all made to press freedom and the challenges posed by new contingencies and new technology, but these cannot be left at the level of rhetorical gestures"
(President Michael D Higgins]

Revelations in January, 2016 that the Garda Services Ombudsman Commission had authorised its investigators to demand access to the mobile 'phone records of two journalists on foot of its powers under section 98 of the Garda Síochána Act, exercised in the context of a disclosure request for telephone records made under section 6 of the Communications (Retention of Data) Act, 2011, have given rise to this Ministerial Review.

In response to those revelations, National Union of Journalists (NUJ) representatives met the Minister for Justice, Equality and Law Reform. NUJ representatives also met the Garda Síochána Ombudsman Commission (GSOC).

Mr Justice John Murray has now been requested by the Minister for Justice; "*to examine the legislative framework in respect to access by statutory bodies to communications data of journalists held by communications service providers, taking into account the principle of protection of journalistic sources; the need for statutory bodies with investigative/and or prosecution powers to have access to data in order to prevent and detect serious crime; and current best international practice in this area*".

This submission articulates and expands upon the firmly held view of the NUJ that the highest level of protection, under both Irish Constitutional and international law, must be afforded to journalists in respect of privacy in their communications in light of the crucial role of the media in maintaining accountability and transparency in the workings of civic society in a democratic state.

While there is an individual right of privacy afforded to citizens the right of privacy afforded to journalists in the exercise of their professional function is rooted in a public good that extends beyond the individual rights of citizens.

1. The right to privacy in communications.

GLOBAL

Universal Declaration of Human Rights
Article 12

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

The dangers to society and individual rights posed by the potential for State interception of digital communications generally were explicitly addressed by United Nations Resolution no. 68/167, on *The Right to Privacy in the Digital Age*, adopted by the General Assembly on 18 December 2013 as demonstrated by the following extract from the Resolution:

"The General Assembly,
...
4. *Calls upon* all States:
...
(*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

In October 2000, the Organization of American States (OAS) adopted the Declaration of Principles on Freedom of Expression. Principle 8 states:

"Every social communicator has the right to keep his/her source of information, notes, personal and professional archives confidential."

NATIONAL / DOMESTIC

The un-enumerated implicit constitutional right to privacy afforded citizens by Bunreacht na hÉireann has been unequivocally held by the courts to extend to privacy in communications. (*Kennedy and Ors v Ireland [1987] IR 587).*

Geraldine Kennedy and Bruce Arnold, both then NUJ members and political journalists, successfully established in the High Court the Constitutional right to privacy in communications of all citizens subject always to lawful exceptions which were found not to have applied in respect of the tapping of their private telephones by the State.

E Privacy Regulations, 2011

European Communities (Electronic Communications Networks and Services) Privacy and Electronic Communications) Regulations, 2011 (SI336/2011) implementing the EU E Privacy Directive (Directive 2009/136/EC). This purpose of these Regulations is to impose security and data protection obligations on electronic communications networks and services

providers in order to safeguard the privacy of communications of users of those networks and services.

EUROPEAN

The right of privacy in communication is recognised explicitly by Article 8 of the European Convention on Human Rights:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

This right was most recently upheld in favour of a journalist in the European Court of Human Rights (ECtHR) Grand Chamber decision in *Roman Zakharov v Russia (Application 47143/06) of* 04 December, 2014. The judgment emphasizes the proportionality principle in any interference with an individual's right of privacy in their communications. It also addresses the desirability of informed judicial oversight of any system of interception by State authorities of an individual's telecommunications.

While that case turns on its own facts, it is submitted that the judgment of the Court merits consideration in the context of this Review. Extracts deemed particularly relevant to the deliberations of this Review are set out in Appendix 1. One sentence stands out: "*In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court [ECtHR] must be satisfied that there are adequate and effective guarantees against abuse." (para. 232).*

It is this consideration of the effects of secretly accessing data concerning journalists' telephone communications on the effective functioning of the media and on the effective functioning of democracy itself, that calls for exceptional levels of protection to be extended to the private communications of journalists.

E Privacy Directive of 2009

The EU E Privacy Directive (Directive 2009/136/EC) was incorporated into Irish domestic law by the European Communities (Electronic Communications Networks and Services) Privacy and Electronic Communications) Regulations, 2011 (SI336/2011) This purpose of this Directive is to impose security and data protection obligations on electronic communications networks and services providers in order to safeguard the privacy of communications of users of those networks and services.

2. The right to freedom of expression

GLOBAL

Universal Declaration of Human Rights
Article 19

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

The International Covenant on Civil and Political Rights (ICCPR) committing signatory states to upholding the rights set out in the Universal Declaration of Human Rights was signed by Ireland in 1989.

NATIONAL / DOMESTIC

The explicit constitutional right to freely express convictions and opinions provided for citizens by Article 40.6.1° of Bunreacht na hÉireann has been upheld by the Irish Courts consistently in the context of appeals brought by media outlets and journalists.

The right to freedom of expression was expressed by Barrington J in the Supreme Court in *Irish Times v Ireland [1998] 1 IR 359 (at p.405)* to be *"a right to communicate facts as well as a right to comment on them".*

Fennelly J in the Supreme Court in *Mahon v Post Publications [2007] IESC 15* held that restrictions imposed by the Mahon Tribunal on the publication of certain information that had been submitted to the Tribunal were disproportionate, to the extent that they interfered both with the Constitutional right to freedom of expression enjoyed by the media and the similar right afforded by Article 10 of the European Convention on Human Rights At para. 51 of his judgment, he stated, "*The right of a free press to communicate information without let or restraint is intrinsic to a free and democratic society*". Significantly, he states at para. 43 of his judgment that the *"right of freedom of expression extends the same protection to worthless, prurient and meretricious publication as it does to worthy, serious and socially valuable works".*

EUROPEAN

European Convention on Human Rights
Article 10 – Freedom of Expression

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

There is extensive case law from the European Court of Human Rights (ECtHR) exploring the parameters of what constitutes restrictions that are '*necessary in a democratic society'* in the interests listed in Article 10.2. Provided here is a hyperlink to a useful and concise summary of recent ECtHR case law on Article 10 prepared by the ECtHR: http://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf

The provisions of the Convention were effectively incorporated into domestic law by virtue of the European Convention on Human Rights Act, 2003. The 2003 Acts requires that every organ of the State carry out its functions in a manner compatible with the State's obligations under the Convention (section 3). Further, a court, when interpreting and applying Convention provisions, is required to take 'due account' of principles laid down *inter alia* in decisions of the ECtHR (section 4).

The Council of Europe has consistently recognised the right to freedom of expression and has sought to balance rights.

At the 4th European Ministerial Conference on Mass Media Policy - Prague, 7-8 December 1994, Resolution No 2 noted:

"Principle 2
The practice of journalism in the different electronic and print media is rooted in particular in the fundamental right to freedom of expression guaranteed by Article 10 of the European Convention on Human Rights, as interpreted through the case law of the Convention's organs.

Principle 3
The following enables journalism to contribute to the maintenance and development of genuine democracy:

a) unrestricted access to the journalistic profession;

b) genuine editorial independence vis-à-vis political power and pressures exerted by private interest groups or by public authorities;

c) access to information held by public authorities, granted on an equitable and impartial basis, in the pursuit of an open information policy;

d) the protection of the confidentiality of the sources used by journalists.

The concluding documents of the 1986 Vienna meeting of the OSCE committed member states to… ensure that, in pursuing this activity, journalists, including those representing media from other participating States, are free to seek access to and maintain contacts with public and private sources of information and that their need for professional confidentiality is respected."

Setting the bar for any interference with the exercise of the right of freedom of expression by journalists

The bar on any measure that could undermine the communication of facts and opinions of social and political importance to the public, or indeed that could undermine the right of freedom of expression in material that does not carry any significant degree of social and political importance at all, must of necessity be set particularly high to ensure that the Constitutional and internationally-recognised right of freedom of expression of the media is fully protected. This imperative is emphasised in the interests of our society as a functioning democracy and not solely in the interests of journalists as individual members of that society.

3. Protection of confidentiality of journalists' sources

Protection of the confidentiality of their sources is a core principle for all journalists. This principle is enshrined in the NUJ Code of Conduct (see Appendix 2) the relevant provisions of which state:

A Journalist…..

(1*) At all times upholds and defends the principle of media freedom, the right of freedom of expression and the right of the public to be informed.*

(7) Protects the identity of sources who supply information in confidence and material gathered in the course of her/his work.

In the print industry the majority of journalists in the Republic of Ireland work for media organisations affiliated to the Press Council of Ireland (PCI) and consequently are also required to adhere to the Code of Practice of the PCI (see Appendix 3).

In the context of the terms of reference of this Review attention is drawn to Principle 6 of the Code of Practice of the PCI:

Principle 6 − Protection of Sources: Journalists shall protect confidential sources of information.

The necessity to protect the anonymity of journalists' sources is critical to the disclosure, through a journalist, of information that requires to be released into the public domain where the peril of the disclosure to the informant is such that the information can only be disclosed on the assurance of anonymity.

The commitment of journalists to maintaining the anonymity of their sources has been demonstrated time and again in the actions of journalists across the world willing to endure the risk and on occasion the actuality of imprisonment, rather than disclose the identity of their anonymous sources.

See for example the case of Judith Miller of the New York Times in 2005 (http://www.nytimes.com/2005/07/07/opinion/judith-miller-goes-to-jail.html?_r=0) ; in this jurisdiction Kevin O'Kelly of RTÉ in 1972 (http://www.rte.ie/archives/profiles/okelly-kevin/) and Barry O'Kelly in 1997(http://www.irishtimes.com/news/judge-declines-to-jail-journalist-who-refused-to-name-informant-1.21591) ; in Northern Ireland Ed Moloney in Belfast Appeal Court in 1999 (reversing on appeal an order that Moloney hand over to the RUC interview notes of an interview with UDA paramilitary William Stobie).

The principle of the protection of journalists' sources was most recently considered in the Irish courts in *Mahon v Keena and Kennedy [2009] IESC 64.*

In the Supreme Court judgment on the appeal against a High Court ruling requiring Irish Times editor, Geraldine Kennedy and journalist Colm Keena to answer questions of the Mahon Tribunal on the source of certain information published in the Irish Times, Fennelly J, having observed that the right to freedom of expression may be subject to legitimate restrictions, stated at para. 49;

"Nonetheless, the [ECtHR] constantly emphasises the value of a free press as one of the essential foundations of a democratic society, that the press generates and promotes political debate, informs the public in time of elections, scrutinises the behaviour of governments and public officials and, for these reasons, that persons in public life must expect to be subjected to disclosure about their financial and other affairs, to criticism and to less favourable treatment than those in private life. Generally, therefore, restrictions on freedom of expression must be justified by an "overriding requirement in the public interest.""

Discussing the ECtHR judgment in the *Goodwin* case (see below) and quoting from that judgment, Fennelly J observed towards the end of para. 52;

"Ultimately, the court considered that the interests protected by that Article 10 "tip the balance of competing interests in favour of the interest of Democratic society in securing a free press" and that "the residual threat of damage through dissemination of the confidential information otherwise than by the press, in obtaining compensation and in unmasking a disloyal employee or collaborator were, even if considered cumulatively, not sufficient to outweigh the vital public interest in the protection of the applicant journalist's source.""

The touchstone case informing the jurisprudence of the ECtHR on the protection of journalists' sources, and referenced in the *Mahon v Keena* judgment, was and remains *Goodwin v United Kingdom ECtHR (Application 17488/90)* of 27 March, 1996. The NUJ

supported our member, William Goodwin, in his successful claim to vindicate of his journalistic right to maintain the confidentiality of his sources.

Goodwin recognises the core importance of balancing the public interest served by encouraging the flow of information to journalists by sources who may wish to remain anonymous against the confidentiality of the information disclosed. While the entirety of the judgment has direct and fundamental relevance to the deliberations of this Review, the view of the ECtHR as expressed at para. 39 is set out below:

"The Court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance (see, as a recent authority, the Jersild v. Denmark judgment of 23 September 1994, Series A no. 298, p. 23, para. 31).
Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest."

A hyperlink to a concise and comprehensive article appearing on the website of Article 19, a respected international organisation working to protect and vindicate the right to freedom of expression recognised by Article 19 of the Universal Declaration of Human Rights, which addresses the issue of protection of journalists' sources internationally, is provided here https://www.article19.org/pages/en/protection-of-sources-more.html

4. Data Protection Legislation

Section 22A of the Data Protection Act, 1988 (as amended) recognises the need in the public interest to exempt what would otherwise be 'personal data' subject to the rules of data protection from those rules, where that information is held for the purposes of journalistic publication in the public interest:

22A. (1) Personal data that are processed only for journalistic, artistic or literary purposes shall be exempt from compliance with any provision of this Act specified in subsection (2) of the section if -

(a) the processing is undertaken solely with a view to the publication of any journalistic, literary or artistic material,

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, such publication would be in the public interest, and

(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision would be incompatible with journalistic, artistic or literary purposes.

This principle, which applies across the EU, recognises that there is a need to treat confidential information held for journalistic purposes as a special category of information attracting special protections under the law.

5. The balancing of rights

The decision as to whether or not to permit State investigation authorities access to information concerning the private communications of journalists is, as is clear from the over-view of the relevant domestic and international law set out in this submission, one that requires a careful, considered and informed balancing of fundamental constitutional and civil rights.

The NUJ notes with deep concern, that the recent exercise by GSOC of its section 98 power to demand disclosure of telecommunications data concerning our members' private telephone communications, was exercised in the context of an investigation into a suspected criminal offence that is arguably on the borderline of the level of 'seriousness' required to merit the exercise of the power to seek disclosure under section 6 of the Communications (Retention of Data) Act, 2011.

The 2011 Act grants the power to a member of An Garda Síochána, not below the rank of Chief Superintendent, to make a disclosure request where she / he is satisfied that the disclosure is required for:

(a) the prevention, detection, investigation or prosecution of a serious offence,
(b) the safeguarding of the security of the State,
(c) the saving of human life.

The 2011 Act defines a 'serious offence' as one that is punishable by imprisonment of 5 years or more (together with a handful of offences set out in Schedule 1 to the Act that are not relevant to this discussion).

The suspected criminal offence in respect of which disclosure requests were made on the authority of GSOC was not one that was committed (if committed at all) by the journalists whose 'phone data was accessed. It was a suspected offence that, if committed at all, was committed 8 years ago and which, if a conviction ensued, would attract penalties:

- on summary conviction – fine up to €3,000 and maximum 12 months' imprisonment (or both)
- on conviction on indictment – fine up to €50,000 and maximum 5 years' imprisonment (or both)

In the event that a gift or consideration was accepted by the offending Garda for disclosing information to the media, the penalties on indictment rises to maximum fine of €75,000 and maximum 7 years' imprisonment (or both).

It is submitted that the suspected offence being investigated was, while a criminal offence, towards the lower end of the scale of serious offences as defined by the 2011 Act. Further, it must be queried how the process of carrying out the necessary balancing of potentially competing Constitutional and civil rights was addressed by GSOC prior to its authorisation of the disclosure request that led to such a profoundly serious and worrying encroachment on the rights of the journalists in question.

While the National Union of Journalists held a meeting with GSOC the Commissioners said they were unable to discuss specific incidents.

6. Practical implications for journalists

The NUJ represents full-time journalists employed in the print, electronic and on-line media, working in diverse range of media organisations and platforms either as employees or freelance workers and contributors.

1. The NUJ has long asserted the right of journalists to refuse to divulge both the names of their sources and the nature of the information conveyed to them in confidence. As stated earlier in this submission, the NUJ actively supported William Goodwin in his successful application to the ECtHR in 1996 to vindicate his right to freedom of expression in the face of an Order from the UK courts that he disclose confidential sources of a business article he had written.

2. A free and effective media depends on the free flow of information to journalists, often from sources that may wish for various reasons to remain anonymous. Respect for that anonymity can often be a precondition for the supply of information provided by sources in the public interest. Journalists are trained and experienced in evaluating information received from such sources.

3. The protection of confidential information about sources from public disclosure is the cornerstone of investigative journalism. Any statutory provision that potentially undermines such protection inevitably inhibits the ability of journalists and media organisations to carry out their work in the public interest.

4. The ability of journalists to expose corruption or wrongdoing is compromised when the protection of the confidentiality sources is put at risk. To have in place laws that enable a State official to authorise actions that clearly put the confidentiality of sources at risk, despite journalistic commitments to honour that confidentiality, cannot but undermine public confidence in the capacity of journalists to deliver on such commitments.

5. The chilling effect of routine, non-judicially authorised accessing of data held by journalists can only deter whistle-blowers from contacting journalists. It further has the ominous potential to promote a culture of secrecy within our system of politics and public administration.

6. The accessing of communications data held by journalists has profound implications for the profession of journalism. A journalist whose confidential sources have been compromised, for example on foot of their private communications data being accessed by a state authority, is at serious risk of suffering 'career blight'. The trust carefully developed over years with a wide range of contacts can be obliterated at a stroke by such actions by a state authority.

7. Summary of NUJ submissions to Review

Based on the law, the principles discussed in this submission and the practical implications for a free media and the practice of journalism of involuntary / forced disclosure of information about journalists' confidential sources, the NUJ submits to this Review as follows:

1. Secret access to a journalist's private communications data on the authority of a State official, not exercising judicial authority and with no opportunity for the journalist to challenge the proposed disclosure, is disproportionate, oppressive, contrary to the public interest and contrary to democratic principles enshrined in the Constitution and protected by international treaties of which Ireland is a signatory.

2. The profound implications for society generally as well as the individual journalists concerned, requires that any authorisation by a member of An Garda Síochána or other State official to seek disclosure of journalists' confidential communications or other private data should be carried out only by a person exercising judicial authority.

3. Wherever feasible, the journalist in question should have prior notice of the proposed request for disclosure and be afforded the right to make representations to the court on the application being made by a State authority / official.

4. By reference to established European law and also Irish law, any order issued with legal authority, which compels journalists to answer questions for the purpose of identifying their source or accesses that information without their knowledge, can only be justified by an overriding requirement in the public interest. Such overriding requirement, it is submitted, must be more than a mere convenience for criminal investigation authorities. Of necessity, the deleterious consequences for journalism

and freedom of expression must be weighed against the advantages to criminal investigation authorities of such orders or disclosures.

5. The current tendency by An Garda Siochána to routinely seek access to notes and images held by journalists can fly in the face of the principle of 'overriding requirement in the public interest' as justification for such disclosures. News organisations report frequent visits to their offices and requests for interviews with reporters and journalists, even where material requested is already in the public domain. Photographers frequently receive demands to hand over data such as images readily available from CCTV cameras at public events., including public protests and demonstrations.

6. The NUJ is aware that some news organisations have handed over information, in order to avoid a costly court challenge and to avoid drawing public attention to the inherent threat to maintaining the confidentiality of sources. The NUJ views this tendency with alarm, due to the potential 'chilling effect' of such actions and the consequences of such effect for the environment in which journalists in this jurisdiction operate.

7. In *Mahon v Kennedy and Keena* the Supreme Court held that the exercise of balancing competing constitutional rights is entirely a matter for the courts, not journalists; a view endorsed emphatically by the EctHR in a subsequent application by those journalists to that court in respect of the costs award made against them in the case. The NUJ contends that the converse is true in that it is not a matter for a senior ranking Garda or a member of GSOC to decide whether or not there the required level of overriding public interest is present to merit access to journalists' private data. There should properly be recourse to a judicial authority to do so.

The NUJ thanks Mr Justice Murray for his kind attention and consideration of this submission. The NUJ would be pleased to provide any further explanation or expansion on its position as set out in this submission.

Seamus Dooley,
Irish Secretary, NUJ
11 March, 2016

APPENDIX 1

EXTRACT FROM GRAND CHAMBER JUDGMENT OF EUROPEAN COURT OF HUMAN RIGHTS IN ROMAN ZAKHAROV V RUSSIA (APPLICATION 47143/06); 04.12.15

"230. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

231. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Amann v. Switzerland* [GC], no. 27798/95, §§ 56-58, ECHR 2000‑ II; *Valenzuela Contreras*, cited above, § 46; *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev,* cited above, § 76).

232. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Klass and Others*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106; *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009; and *Kennedy*, cited above, §§ 153 and 154).

APPENDIX 2

NUJ Code of Conduct

A journalist:

1 At all times upholds and defends the principle of media freedom, the right of freedom of expression and the right of the public to be informed.

2 Strives to ensure that information disseminated is honestly conveyed, accurate and fair.

3 Does her/his utmost to correct harmful inaccuracies.

4 Differentiates between fact and opinion.

5 Obtains material by honest, straightforward and open means, with the exception of investigations that are both overwhelmingly in the public interest and which involve evidence that cannot be obtained by straightforward means.

6 Does nothing to intrude into anybody's private life, grief or distress unless justified by overriding consideration of the public interest.

7 Protects the identity of sources who supply information in confidence and material gathered in the course of her/his work.

8 Resists threats or any other inducements to influence, distort or suppress information and takes no unfair personal advantage of information gained in the course of her/his duties before the information is public knowledge.

9 Produces no material likely to lead to hatred or discrimination on the grounds of a person's age, gender, race, colour, creed, legal status, disability, marital status, or sexual orientation.

10 Does not by way of statement, voice or appearance endorse by advertisement any commercial product or service save for the promotion of her/his own work or of the medium by which she/he is employed.

11 A journalist shall normally seek the consent of an appropriate adult when interviewing or photographing a child for a story about her/his welfare.

12 Avoids plagiarism.

The NUJ believes a journalist has the right to refuse an assignment or be identified as the author of editorial that would break the letter or spirit of the NUJ code of conduct.

The NUJ will support journalists who act according to the code.

NUJ code of conduct was updated in 2011.

APPENDIX 3
Press Council of Ireland Code of Practice

Preamble
The freedom to publish is vital to the right of the people to be informed. This freedom includes the right of a print and online news media to publish what it considers to be news, without fear or favour, and the right to comment upon it.

Freedom of the press carries responsibilities. Members of the press have a duty to maintain the highest professional and ethical standards.

This Code sets the benchmark for those standards. It is the duty of the Press Ombudsman and Press Council of Ireland to ensure that it is honoured in the spirit as well as in the letter, and it is the duty of publications to assist them in that task.

In dealing with complaints, the Ombudsman and Press Council will give consideration to what they perceive to be the public interest. It is for them to define the public interest in each case, but the general principle is that the public interest is invoked in relation to a matter capable of affecting the people at large so that they may legitimately be interested in receiving and the print and online news media legitimately interested in providing information about it.

Principle 1 − Truth and Accuracy

1.1 In reporting news and information, print and online news media shall strive at all times for truth and accuracy.

1.2 When a significant inaccuracy, misleading statement or distorted report or picture has been published, it shall be corrected promptly and with due prominence.

1.3 When appropriate, a retraction, apology, clarification, explanation or response shall be published promptly and with due prominence.

Principle 2 − Distinguishing Fact and Comment

2.1 Print and online news media are entitled to advocate strongly their own views on topics.

2.2 Comment, conjecture, rumour and unconfirmed reports shall not be reported as if they were fact.

2.3 Readers are entitled to expect that the content of a publication reflects the best judgment of editors and writers and has not been inappropriately influenced by undisclosed interests. Wherever relevant, any significant financial interest of an organization should be disclosed. Writers should disclose significant potential conflicts of interest to their editors.

Principle 3 − Fair Procedures and Honesty

3.1 Print and online news media shall strive at all times for fair procedures and honesty in the procuring and publishing of news and information.

3.2 Publications shall not obtain information, photographs or other material through misrepresentation or subterfuge, unless justified by the public interest.

3.3 Journalists and photographers must not obtain, or seek to obtain, information and

photographs through harassment, unless their actions are justified in the public interest.

Principle 4 − Respect for Rights

4.1 Everyone has constitutional protection for his or her good name. Print and online news media shall not knowingly publish matter based on malicious misrepresentation or unfounded accusations, and must take reasonable care in checking facts before publication.

Principle 5 − Privacy

5.1 Privacy is a human right, protected as a personal right in the Irish Constitution and the European Convention on Human Rights, which is incorporated into Irish law. The private and family life, home and correspondence of everyone must be respected.

5.2 Readers are entitled to have news and comment presented with respect for the privacy and sensibilities of individuals. However, the right to privacy should not prevent publication of matters of public record or in the public interest.

5.3 Sympathy and discretion must be shown at all times in seeking information in situations of personal grief or shock. In publishing such information, the feelings of grieving families should be taken into account. This should not be interpreted as restricting the right to report judicial proceedings.

5.4 In the reporting of suicide excessive detail of the means of suicide should be avoided.

5.5 Public persons are entitled to privacy. However, where a person holds public office, deals with public affairs, follows a public career, or has sought or obtained publicity for his activities, publication of relevant details of his private life and circumstances may be justifiable where the information revealed relates to the validity of the persons conduct, the credibility of his public statements, the value of his publicly expressed views or is otherwise in the public interest.

5.6 Taking photographs of individuals in private places without their consent is not acceptable, unless justified by the public interest.

Principle 6 − Protection of Sources

Journalists shall protect confidential sources of information.

Principle 7 − Court Reporting

Print and Online news media shall strive to ensure that court reports (including the use of images) are fair and accurate, are not prejudicial to the right to a fair trial and that the presumption of innocence is respected.

Principle 8 − Prejudice

Print and online news media shall not publish material intended or likely to cause grave offence or stir up hatred against an individual or group on the basis of their race, religion, nationality, colour, ethnic origin, membership of the travelling community, gender, sexual orientation, marital status, disability, illness or age.

Principle 9 − Children

9.1 Print and online news media shall take particular care in seeking and presenting information or comment about a child under the age of 16.

9.2 Journalists and editors should have regard for the vulnerability of children, and in all dealings with children should bear in mind the age of the child, whether parental or other adult consent has been obtained for such dealings, the sensitivity of the subject-matter, and what circumstances if any make the story one of public interest. Young people should be free to complete their time at school without unnecessary intrusion. The fame, notoriety or position of a parent or guardian must not be used as sole justification for publishing details of a child's private life.

Principle 10 − Publication of the Decision of the Press Ombudsman / Press Council

10.1 When requested or required by the Press Ombudsman and/or the Press Council to do so, print and online media shall publish the decision in relation to a complaint with due prominence.

10.2 The content of this Code will be reviewed at regular intervals.