Submission to the

Review by Mr Justice John L. Murray

of the Law on Access to Communications Data

Introduction

1. The Irish Council for Civil Liberties (ICCL) is Ireland's leading independent human rights watchdog, which monitors, educates and campaigns in order to secure full enjoyment of human rights for everyone.

2. In January 2016, Mr Justice John L Murray was appointed by the Minister for Justice and Equality to undertake an independent review into the use of data retention powers to access communications records of journalists. The review was established following revelations in the media that the Garda Síochána Ombudsman Commission (GSOC) had, during the course of an investigation into the suspected leaking of information to the media by members of An Garda Síochána, accessed the phone records of a number of journalists. It is understood that the review will focus on the relevant provisions of the Communications (Retention of Data) Act 2011.

Terms of Reference

3. The Terms of Reference established for the review are:

> *'To examine the legislative framework in respect of 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.'*

Legal Framework Governing Privacy

International Human Rights Obligations

4. The right to privacy is protected by a number of international treaties by which Ireland is bound including the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and the International Covenant on Civil and Political Rights (ICCPR).

European Union Law

5. Ireland is also bound by the provisions of Article 7 (the right to privacy) and Article 8 (the protection of personal data) of the Charter of Fundamental Rights of the European Union. On 8 April 2014, the Court of Justice of European Union struck down the *EU Data Retention Directive (2006/24/EC)* as invalid (cases of *Digital Rights Ireland v. Minister for Communications, Minister for Justice and Equality, Commissioner of The Garda Síochána, Ireland and the Attorney General* (C-293/12); *Karnter Landesregierung, Michael Seitlinger, Christof Tschohl and Others* (C-594-12). The Court found that the Directive amounted to a disproportionate interference with the fundamental rights to respect for individual privacy and the protection of personal data guaranteed by Articles 7 and 8 of the Charter. The decision will require EU Member States to reconsider national laws transposing the Directive and will result in the introduction of new legislation to replace the invalidated Directive. To date that legislation has not been adopted.

6. The EU ePrivacy Directive 2002/58/EC has been given effect in Irish Law by the ePrivacy Regulations 2011. The regulations cover data protection for data transmitted and received via telephone, e-mail and the internet.

7. The EU Data Protection Directive 95/46/EC, together with the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, has been given effect in Irish law by the passage of the Data Protection Acts 1988 and 2003.

European Convention on Human Rights

8. The European Convention on Human Rights (ECHR) guarantees certain rights to individuals and has been given further effect in Irish law by the European Convention on Human Rights Act 2003.

   Article 8 of the Convention provides:

   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 it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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.*

9. The European Court of Human Rights (ECtHR) has found that the right to privacy includes the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; and informational privacy, including online information (*Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I). The Court has

also found that "in determining whether the personal information retained by the authorities involves any ... private life [aspect] ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ..." (*S. and Marper v. the United Kingdom* nos. 30562/04 and 30566/04, 4 December 2008)

10. The Court has also considered the issue of storage and use of personal data and has opined that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8. It found that domestic law must afford appropriate safeguards to prevent use of such data as may be inconsistent with the guarantees of Article 8 and, in particular, that "adequate guarantees that retained personal data were efficiently protected from misuse and abuse" are in place (*S. and Marper v. the United Kingdom* nos. 30562/04 and 30566/04, 4 December 2008). The Court has noted that the need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, "not least when such data are used for police purposes."

11. In relation to the substantive issue of the protection of journalistic sources, the Court has found that domestic law must provide appropriate safeguards in relation to powers of surveillance with a view to uncovering journalistic sources in order to guarantee the protections contained in Article 8 and Article 10 (Freedom of Expression) of the Convention. The Court has further noted the importance of protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order for source disclosure could have on the exercise of that freedom (*Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands* no. 39315/06, 22 November 2012).

12. The Court has also found that in order to interfere with an applicant's freedom of expression as guaranteed under article 10 to identify journalistic sources, there must be a procedure prescribed by law setting out adequate legal safeguards available to the applicant to enable an independent assessment as to whether the interest of a criminal investigation overrode the public interest in the protection of journalistic sources (*Sanoma Uitgevers B.V. v. the Netherlands* no. 38224/03 14 September 2010).

International Covenant on Civil and Political Rights

13. Ireland is also bound by the International Covenant on Civil and Political Rights (ICCPR) which it has signed and ratified. Article 17 of ICCPR provides that "*no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*". In its interpretation of Article 17 the UN Human Rights Committee has identified a positive obligation on states parties to the Covenant to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."

Irish Domestic Law

14. The right to privacy is guaranteed under Irish law having been identified as an unenumerated right protected under Article 40.1 the Irish Constitution (*Kennedy and Arnold v. Attorney General* [1987] IR 587. The right to privacy extends to communications by telephone, email and the internet.

15. In relation to the protection of journalistic sources in Irish law, the Supreme Court has upheld the right of journalists to protect their sources (*Mahon Tribunal v Keena and Anor* [2009] IESC 64).

16. **The ICCL recommends that in reviewing the legislative framework governing data retention law in Ireland Judge Murray gives due consideration not only to domestic law but also to the obligations on the State arising from Ireland's status as a party to relevant International treaty bodies and human rights instruments including, but not limited to, the EU Charter of Fundamental Rights, the European Convention on Human Rights and the International Covenant on Civil and Political Rights.**

Powers of Gardaí and GSOC under the Communications (Retention of Data) Act 2011

17. Access to retained communications data by certain statutory agencies is made by way of a disclosure request. Provisions for making a disclosure request are governed by section 6 of the Communications (Retention of Data) Act 2011. Under Section 6(1) a member of An Garda Síochána not below the rank of superintendent, an officer of the Permanent Defence Force not below the rank of Colonel (section 6(2)) and an officer of the Revenue Commissioners not below the rank of Principal Officer (section 6(3)) may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 of the Act where that member is satisfied that the data are required for (a) the prevention, detection, investigation or prosecution of a serious offence, (b) the safeguarding of the security of the State, and / or (c) the saving of human life. The legislation provides that a disclosure request must be made in writing, but that this provision may be dispensed with in cases of exceptional urgency in which case the request may be made orally (whether by telephone or otherwise) by a person so entitled under the Act. Section 6(5) provides that an oral request must be confirmed in writing to the service provider within two working days of the request being made.

18. The powers outlined above are also available to members of GSOC in the course of investigating a suspected offence. Under section 98(1) of the Garda Síochána Act 2005, a designated officer of GSOC who is directed by the Ombudsman to investigate a complaint under this section has "in relation to the member of the Garda Síochána under investigation, for the purposes of the investigation all the powers, immunities and privileges conferred all the duties imposed on any member of the Garda Síochána by or under any enactment or the common law…" This means that the powers conferred on members of An Garda Síochána under the Communications (Retention of Data) Act 2011 are also conferred upon members of GSOC acting in the course of a criminal investigation.

19. Section 98(1) of the 2005 Act also compels GSOC to produce a report to the Minister in accordance with Section 9(1) of the 2011 Act in respect of data that were the subject of all disclosure requests made under section 6 (1) during the relevant period with the report to be submitted as soon as is practicable after the end of that period. The information contained in this report is specified under section 9(5) to include only (a) the number of times when data had been disclosed in response to a disclosure request, (b) the number of times when a disclosure request could not be met, and (c) the average period of time between the date on which the retained data were first processed and the disclosure request. Upon receipt of this report, the Minister must produce a State report for submission to the European Commission.

Issue of Self-Authorisation

20. Section 6 of the 2011 Act provides for internal oversight of disclosure requests only. In addition, reports compiled by the relevant authority of each body for submission to the relevant Minister contains only limited statistical data including the number of requests, the number of times requests could not be met and the time between the date the data was first retained and the disclosure request. This means that neither the nature nor the rationale for the request is governed by any external oversight mechanisms.

21. The limited scope of these provisions contrast sharply with a number of provisions governing other types of data access provided in legislation. For example, Section 4 of the Surveillance Act 2009 requires judicial authorisation to be sought prior to the use of surveillance devices (e.g. audio bugging devices, video cameras, etc.) by authorised personnel. Such authorisation is only granted in relation to arrestable offences i.e. offences which carry a penalty of 5 or more years of imprisonment. The provisions of the 2009 Act provide a significant number of protections that are not provided under the 2011 Act including judicial oversight, specific criteria governing authorisation, including the nature and type of an offence, justification and safeguards governing the granting of authorisation and self-authorisation. By contrast, the 2011 Act which lacks equivalent safeguards.

22. It is the view of the ICCL that significant reform of the Communications (Data Retention) Act 2011 is required to ensure that the legislation provides a measure of judicial oversight comparable with existing legislation.

23. **The ICCL recommends that legislation governing access by statutory agencies to retained data including but not limited to the Communications (Data Retention) Act 2011 include provisions to ensure, where appropriate, judicial oversight of disclosure requests.**

24. **The ICCL recommends that specific criteria governing the application for disclosure requests relate only to certain categories of suspected offences already defined in**

legislation governing surveillance and other matters and that such applications must be shown to be justified and proportionate.

25. The ICCL also notes that the legislative framework in question is used by a number of law enforcement agencies to capture a wide range of private information about members of the public and is not confined to journalists. As a result, the oversight shortcomings that this review is likely to identify will not be confined to cases where the data belongs to members of the media but also to the general public.
