Submission to Joint Committee on Justice and Equality
Communications (Retention of Data) Act Bill 2017
General Scheme Pre-legislative Scrutiny
16th November 2017[1]

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:

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.[2]

Strict Necessity. 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'.[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 likely to

[1] The following is an updated version of submissions made by Digital Rights Ireland and the Irish Council for Civil Liberties to the Oireachtas Committee on Justice and Equality on November 8 and 15.
[2] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at paras 402 - 408.
[3] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.

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'.[4]

A Limited Retention Period. Uphold the requirements of *Tele2* that a Ministerial Order for Data Retention must be limited to what is strictly necessary[5] and in any event no more than 3 months.

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.[6]

Precise Definitions of data being collected. 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.

In cases of urgency, 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. [7]

In cases of urgency, require a Judge or Oversight body. Uphold the requirements of *Sanoma* that even urgent situations require independent review by a judge or similar body before information capable of identifying sources is handed over or accessed. [8]

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.

Compensation. Retain the current power under the 2011 Act[9] 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 give their reasons to the person who has applied for an investigation into data retention in the event of their 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.

Establish 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.

---

[4] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Paras.110-111.
[5] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para. 108.
[6] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.119.
[7] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 390.
[8] *Sanoma Uitgevers BV v. the Netherlands*, application 38224/03, 14 September 2010.
[9] Communications (Retention of Data) Act, 2011, 3/2011.

Judicial Remedy. Per the Murray Review, 'bearing in mind the coercive nature character of a data retention system, and the concomitant risk to fundamental rights associated with it, that a statue should expressly provide for an appropriate judicial remedy and associated procedures for breaches of rights, including fundamental rights, occasioned by its operation'.[10]

1. Introduction

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)[11], the Minister for Justice and Equality commissioned an independent review of communications data legislation. Former Chief Justice Mr. John L. Murray headed the Review (*Murray Review*)[12] and gave recommendations for amending legislation.

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 in *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources & Others* (*Digital Rights Ireland*).[13] That challenge against the data retention regime in Ireland was referred by the Irish High Court to the CJEU, which resulted in the invalidation of the EU Data Retention Directive (the Directive)[14]. The subsequent CJEU judgment is *Tele2 Sverige AB v Post-Och Telestyrelsen* (*Tele2*)[15] which, building on *Digital Rights Ireland*, sets out strict and binding standards which must be met to make any national system of data retention permissible under EU law and the EU Charter of Fundamental Rights.

The General Scheme of the Bill leaves a fragmented system of oversight in place that does not include key recommendations from the *Murray Review*, or requirements of EU Law or ECHR norms addressed in *Tele2* and *Digital Rights Ireland*.

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.

Finally, 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 our 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

[10] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 336.
[11] Communications (Retention of Data) Act, 2011, 3/2011.
[12] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017).
[13] *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources & Others* (Joined cases C-293/12 and C-594/12).
[14] 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
[15] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15.

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. 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:

Protection of Journalist's Sources

Article 10 of the ECHR guarantees protection of journalistic sources, which is described by the European Court of Human Rights (ECtHR) as a structural support for democratic governance.[16] This principle is reflected in the laws and judicial dicta of many democratic states. The Murray Review proceeds in accordance with the principle that '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'.[17]

The General Scheme of the Bill does not provide explicit protection for journalists as recommended by the Murray Review. Nor does it provide a standard of protection for all citizens sufficient to also protect journalist sources according to the requirements of ECtHR. Specifically *Head 11* violates Article 10 by permitting access to information about journalists' sources without judicial authorisation.

We recommend, per the *Murray Review*, that the General Scheme of the Bill:

- Contain an express provision prohibiting access to data for the purpose of identifying a journalist's sources except in accordance with specific circumstances and conditions;
- To access journalists' communication data, allow prior authorisation only from a judge of the High Court or an independent judicial or administrative body (i.e. no authorisation at the level of the District Court and no emergency authorisations within agencies); and
- Permit access to a journalist's communication data 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.[18]

[16] *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.
[17] 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.
[18] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at paras 402 - 408.

Obliging Service Providers to Retain Communications Data

a) Strict Necessity Test Required

EU jurisprudence requires that communications data can only be retained 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'.[19]

In *Tele2,* the CJEU identified that data retention is, in effect, a form of pre-emptive surveillance and therefore set out the higher standard.[20] Mere utility or even proportionality is not sufficient. Necessity therefore 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'.[21]

Under the General Scheme of the Bill, Heads 5 and 6 detailing Ministerial orders fail to meet the standard of strict necessity and instead apply a weaker standard of *proportionality.*

The test is set out in Head 6 states that the Minister may make an order requiring a service provider to retain communication data unless the Minister is satisfied that the retention of the data *is in all the circumstances proportionate* 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.

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.* , 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'.[22]

b) Targeted, not General, Data Retention Required

Tele2 requires that any national data retention rule must be 'targeted', by meeting objective criteria that establish a connection between the data and objective pursued:

> '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

[19] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.
[20] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at paras. 96, 107 - 110
[21] Cited in Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para 209.
[22] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para.108.

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'.[23]

Under the General Scheme of the Bill, 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 the General Scheme be amended to ensure that any data retention order is targeted according to the terms required by *Tele2*.

c) Limit Retention Period to time strictly necessary time frame

Tele2 requires that when fighting serious crime, the data retention period adopted should be limited 'to what is strictly necessary'.[24]

Under the General Scheme of the Bill, Heads 6 and 7 provides 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 this Head fails to meet the requirement in *Tele2* that 'the retention period adopted [must be limited] to what is strictly necessary'.

We recommend modifying head 7 to provide that Service Providers must store the relevant data for the period specified by the Minister. We also recommend modifying Head 6 beto provide that a data retention order be limited to what is strictly necessary and in any event no more than 3 months.

Third Parties

The standard for *access to data of third parties* – i.e. those not involved in any wrongdoing - is too permissive. In relation to the investigation of serious crime, *Tele2* notes 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 crime or of being implicated in one way or another in such a crime*'.[25]

Under the General Scheme of the Bill, Heads 8 and 9 fail to impose this limitation. They instead permit access to data of entirely unconnected third parties on the more permissive grounds if '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.'

[23] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Paras.110-111.
[24] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 at Para. 108.
[25] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.119.

We recommend narrowing Heads 8(1), (5), (6) and (7) to limit access to data, in the context of the investigation, etc. of crime, only to persons 'implicated in a crime', whether as a perpetrator, victim or witness.

Definition of Traffic and Location Data

Section 1 of the 2011 Act defines 'data' as traffic data or location data and the related data necessary to identify the subscriber or user.

Under the General Scheme of the Bill, Head 1, 'traffic and location data' is given an exceptionally wide and substantially more permissive definition. It includes any 'data processed for the purpose of sending, receiving or storing a communication by means of an electronic communications network'. The definition is so permissive it could permit Ministerial orders to require ISPs to store information about what sites or individual web-pages were visited by individuals. For example, it could 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. This more permissive definition is therefore 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, yet can often reveal the content of a webpage.

We recommend amending the definition of 'traffic and location data' 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 Schedule 2 of the 2011 Act did previously

Urgency

a) Retrospective Authorisation

The *Murray review* recommended that urgency exceptions provided for in national data retention legislation '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.'[26]

Under the General Scheme of the Bill, Head 11 fails to provide for retrospective authorization when outlining approval to make a disclosure request in cases of urgency.

We recommend, for urgency exceptions to disclosure authorization requirements, mandate restropective authorization to an independent body or designated judge.

[26] Murray J, *Review of the Law on the Retention of and Access to Communications Data* (April 2017) at para. 390.

b) Judicial Authorisation

The ECtHR in *Sanoma Uitgevers BV v. the Netherlands*[27] required 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:

> '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.'[28]

Under the General Scheme of the Bill, Head 11 fails to meet the standards set out by *Sanoma*. It permits information identifying journalists' sources to be accessed in some cases without any judicial approval and instead by a designated agency officer.

We recommend preventing the use of an urgency approval system for information identifying journalists' sources. Always required independent review by a judge or independent body before allowing access to data.

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

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

persons affected to exercise, *inter alia*, their right to a legal remedy... where their rights have been infringed.'[29]

Under the General Scheme of the Bill, Head 15 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 investigations - a formula which makes it clear that what is required is a concrete risk of harm.

We recommend, upholding the requirements of *Tele2* for notification as soon as it is not liable to jeopardise the investigations undertaken.

Designated Judge

Head 18 maintains the existing scheme of oversight by a designated judge of the High Court. We discuss the limitations of this system in section 3 below.

Complaints Procedures

a. Removal of power to order compensation

Under the 2011 Act[30], the Complaints Referee has the power to order that compensation be paid to any person whose personal data was wrongfully disclosed.[31]

Under the General Scheme of the Bill, Head 22 quietly removes this power. Removing compensation requirements would reduce the cost to the state of abuses by forcing complainants to use the more expensive court system 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 modifying subhead (5) to reinstate the power to award compensation provided for in the 2011 Act.

b. ***Restriction on decisions of Complaints Referee***

Under the 2011 Act the Complaint's Referee was not required to give transparent reasons on its decisions. It was instead requied to give formulaic notice in response to a complaint where they find that there has been no contravention

Under the General Scheme of the Bill, Head 22 (6), the Complaints Referee is restricted to essentially the same as the equivalent provision. While the previous Act worked to ensure the the

[29] *Tele2 Sverige AB v Post-Och Telestyrelsen*; C-203/15 and C-698/15 Para.121.
[30] Communications (Retention of Data) Act, 2011, 3/2011.
[31] Communications (Retention of Data) Act 2011, Section 10(5) (b).

blanket secrecy of the fact that communications data had been disclosed, under the Bill there is instead a presumption that individuals will be notified of the fact that their data has been disclosed. Therefore, preventing the Complaints Referee giving its reasons or findings of fact hampers both the complainant and the Complaints Referee's duties under the Bill.

We recommend modifying Head 22 subhead 6 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*

Under the General Scheme of the Bill, Head 21 does not include statistics on the number of complaints made or upheld each year.
We recommend modifying Head 21 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.

3. Institutional Oversight

The CJEU has through a series of judgments held that independent and effective supervision by a Data Protection Agency is an essential component of the right to personal data protection, particularly in the context of surveillance.[32] 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'.[33] 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'.[34] Enshrined monitoring practices by independent bodies like Data Protection Agencies are also recognised to contribute to the development and improvement of internal safeguards in intelligence services.[35] While organised in diverse ways, there are many EU examples, with 16 of the 28 member states including expert bodies overseeing intelligence services.[36]

---

[32] 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).
[33] 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.
[34] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11.
[35] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p56.
[36] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p68.

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

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)[37] 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'.[38] It is at risk of 'over-reliance on the entities supposedly being monitored'.[39] 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.[40]

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'.[41] This is coupled with specific exclusions elsewhere in the legislation.[42] 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

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

[38] 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.

[39] 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.'.

[40] 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.

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

[42] 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.)

telecommunications data[43] – 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'.[44]

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.[45]

Parliamentary Oversight

Ireland and Malta are the only two countries in the EU that do not provide for parliamentary oversight of intelligence activities.[46] 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.[47] 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'.[48]

Parliamentary oversight is crucial precisely because of the secretive nature of security and intelligence activities.[49] 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.[50] The ability of oversight bodies to report directly to parliament (rather than

---

[43] 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.

[44] 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.

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

[46] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p66.

[47] 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

[48] 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.

[49] 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.

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

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.

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.[51] 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.[52]

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.[53] 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).'[54]

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 national standards. The EU FRA's October 2017 report states that 'EU Member States should grant oversight bodies

---

[51] 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/.

[52] 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.

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

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

diverse and technically-qualified professionals'.[55] The ECHR also held in *Klass v Germany* that supervisory mechanisms must be 'vested with sufficient competence to exercise and effective and continuous control'[56] 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.

A number of EU countries explicitly require by law that oversight bodies have internal technical competence.[57] A number of EU expert bodies also recruit external technicians, either on an *ad hoc* or more permanent basis.[58]

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'[59]

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'.[60] 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 therefore recommend that the designated judge be replaced with by a unified independent supervisory authority, with parliamentary accountability, to be chaired by a judge in a nearly full time position, and supported by a secretariat with sufficient technical expertise and financial resources to provide detailed support including formalised public reports.

4. 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

[55] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11.
[56] *Klass v Germany*, Application no 5029/71 (ECtHR, 6 September 1978) para 56
[57] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p12.
[58] A number of EU expert bodies also recruit external technicians, either on an *ad hoc* or more permanent basis (2015), p84
[59] Council of Europe Commissioner for Human Rights (2015), p. 47 - cited in FRA October 2015 report at 43.
[60] European Union Agency for Fundamental Rights report, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (2017), p11

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 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*.

TJ McIntyre Chair Digital Rights Ireland Company Limited by Guarantee 10 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 elizabeth.farries@iccl.ie