''Data retention in the aftermath of Digital Rights Ireland and Seitlinger''

Article · December 2014

CITATIONS
0

READS
339

Maria Helen Murphy
National University of Ireland, Maynooth
18 PUBLICATIONS **35** CITATIONS

This is the draft version of an article later published in the Irish Criminal Law Journal.

This article can be cited as:

Maria Helen Murphy, 'Data retention in the aftermath of *Digital Rights Ireland and Seitlinger*' 24(4) Irish Criminal Law Journal 105

Data retention in the aftermath of *Digital Rights Ireland and Seitlinger*

Bio

Dr Maria Helen Murphy is a Lecturer in Law at NUI, Maynooth. Maria researches in the areas of privacy law, surveillance, information technology law, and human rights.

Abstract

In a high profile decision delivered in April 2014, the Grand Chamber of the Court of Justice of the European Union (CJEU) found the Data Retention Directive[1] to be in breach of the EU Charter of Fundamental Rights (EU Charter).[2] This article examines the impact of the ruling in *Digital Rights Ireland* across the EU and considers how the Irish legislature should respond to this decision in a manner that maintains the appropriate balance between the investigatory aims of the government and the protection of fundamental rights.

Introduction

In a high profile decision delivered in April 2014, the Grand Chamber of the Court of Justice of the European Union (CJEU) found the Data Retention Directive[3] to be in breach of the EU Charter of Fundamental Rights (EU Charter).[4] The decision of the CJEU in *Digital Rights Ireland* was delivered in response to preliminary ruling requests from the Irish High Court and the Austrian Constitutional Court (Verfassungsgerichtshof). The preliminary ruling requests concerned the validity of the Data Retention Directive.[5] The Directive, which had been passed into European Union law in 2006, had mandated that Member States require the retention of all communications metadata for between six and 24 months.[6] The compulsory retention of data

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54.
[2] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164.
[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54.
[4] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164.
[5] Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012. See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney* [2012] O.J. C258/11; Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others [2013] O.J. C79/7.
[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54. The Directive frequently asserted that the "content" of communications cannot be retained under the authority of the Directive. See art. 1(2), art. 5(2), and Recital 13 of the Directive.

under the Directive was introduced as a derogation from the privacy protections established by the Data Protection Directive and the Directive on Privacy and Electronic Communications**.**[7]

In the ruling in *Digital Rights Ireland*, the CJEU criticised the general application of the Directive that required the collection of data on "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made".[8] In line with these criticisms, the CJEU found the Directive to be a disproportionate interference with the EU Charter. The right to respect for private life and the right to protection of personal data as provided for in Articles 7 and 8 of the EU Charter were central to the holding of the Court.[9] The blanket application of the Directive was a particular cause for concern, with the Court pointing out that the Directive "does not require any relationship between the data whose retention is provided for and a threat to public security".[10] This article examines the impact of the ruling in *Digital Rights Ireland* across the EU and considers how the Irish legislature should respond to this decision in a manner that maintains the appropriate balance between the investigatory aims of the government and the protection of fundamental rights.

The Data Retention Directive and the ruling of the CJEU

The primary aim of data retention is articulated in the Data Retention Directive as the "investigation, detection and prosecution of serious crime".[11] As mentioned in the recital to the Directive, the Conclusions of the Justice and Home Affairs Council highlighted the importance of data retention as a valuable tool in not only the investigation, detection and prosecution of crime, but also in the prevention of criminal offences.[12] The Data Retention Directive became law in a political climate of heightened emotion and increased perception of risk following the terrorist attacks in Madrid in 2004 and London in 2005.[13] As argued before the European Parliament by the then UK Home Secretary, Charles Clarke,

> Information is the life-blood of law-enforcement operations and enables our police and agencies to prevent crimes with the minimum of impact on our daily lives. To tackle organised crime and to stop terrorist groups before they carry out activities they need a clear picture of who the criminals are, what they are doing, where they are and how they

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] O.J. L-281; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) [2002] O.J. L-201; Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 32.

[8] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 57.

[9] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 29-30.

[10] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 59.

[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54 art. 1(1).

[12] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 7. The EU policy of mass data retention illustrates an increased focus on anticipatory and preventive investigation in recent times. For general discussion of the movement towards preventive policing and prosecution focused policing see Balkin, "The Constitution in the National Surveillance State" (2008-2009) 93 Minn. L. Rev. 1 at 3-4.

[13] European Council Declaration on Combating Terrorism (March 25, 2004) 7906/04 at 5; European Council Declaration on the EU response to the London bombings (July 13, 2005) 11158/1/05 at at 2; Feiler "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection" (2010) 1 E.J.L.T. 1.

> communicate with each other. Often that picture is pieced together after the fact. But if we are to be effective in dismantling organised crime groups we must analyse intelligence and information so that we can target our efforts on the most dangerous criminals. However, that need is not always reflected in the rules that we apply to our police.[14]

In *Digital Rights Ireland*, the CJEU acknowledged that the fight against terrorism and serious crime constitutes an "objective of general interest".[15] Interestingly, the CJEU also noted that the right to security – as protected by Article 6 of the EU Charter – was also relevant.[16] In spite of the potential that mass data retention offers for the investigation of crime, the CJEU has rejected the argument that the benefits of retention trump the consideration of rights.[17] While the CJEU held that the Data Retention Directive satisfied an objective of general interest, it remained necessary to consider the proportionality of the measures required by the Directive.[18]

In order to assess the arguments of the CJEU, it is necessary to detail the content of the invalidated Directive briefly. The Directive mandated the retention of six specific categories of metadata.[19] Under the Directive, Member States were required to provide for the retention of data that is necessary to determine the source, destination, date, time and duration of a communication. In addition, Member States were obliged to provide for the retention of data necessary to identify the type of communication and the users' communication equipment.[20] The ability of metadata – as opposed to content data – to reveal private information about individuals has, at this point, been well documented.[21] The CJEU showed cognisance of this and stated that the data retained under the Directive had the potential to

> "allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[22]

Citing its own jurisprudence, the CJEU reiterated that the principle of proportionality requires that acts of EU institutions must be appropriate for attaining legitimate objectives, must not

---

[14] Clarke "Speech to the European Parliament" September 7, 2005. Available at http://charlesclarke.org/wp-content/uploads/2011/01/20050907-European-Parliament.rtf; De Goede, "The Politics of Preemption and the War on Terror in Europe" (2008) 14 E.J.I.R. 161.

[15] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 42

[16] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 42

[17] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 51.

[18] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 44-45.

[19] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54 art. (1).

[20] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54 art. (1).

[21] Breyer, "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11 E.L.J. 365 at 365.

[22] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 27. While the CJEU did find the retention of information under the Directive to constitute a "particularly serious interference" with privacy and personal data rights, the CJEU also held that the Directive did not violate "the essence" of those rights. The Court justified this distinction by recognising that the Directive did not permit the retention of content data and the Directive required respect for "certain principles of data protection". Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 39-40.

exceed the limits of what is appropriate, and must be necessary in order to achieve those objectives.[23] While the CJEU recognised that there are several alternative methods of surveillance available to authorities who wish to monitor electronic communications, the Court was clear that data retention could be an appropriate means to achieve the legitimate goals of the Directive.[24] Crucially, even though the CJEU considered the fight against serious crime to be an important objective of the Directive, the Court was clear that a general interest could not, in itself, justify mass data retention.[25] In fact, as the Directive had serious implications for the protection of Articles 7 and 8 of the EU Charter, any limitation of those rights would be justifiable only where "strictly necessary".[26]

Drawing on the case law of the European Court of Human Rights, the CJEU stated that EU legislation mandating data retention must contain

> "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data"[27]

As noted in the introduction to this article, the CJEU criticised the generalised retention of the electronic communications information of every individual irrespective of whether any connection existed between the retained data and serious crime.[28] Specifically, the CJEU criticised the fact that retention was not limited to

> "data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or … to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."[29]

This aspect of the judgment has been highlighted as being of great significance as it implies that the mere retention of information can constitute a breach of the EU Charter when it is carried out indiscriminately. Internal EU documents detailing the proceedings of a closed meeting of the EU Justice and Home Affairs ministers have revealed that the Council's Legal Service believes that this part of the *Digital Rights Ireland* judgment "suggests that general and blanket data

---

[23] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 46. Citing Case C-343/09 *Afton Chemical* [2010] E.U.E.C.J.; Case C-92/09 *Volker und Markus Schecke and Eifert* [2010] E.U.E.C.J.; Joined Cases C-581/10 and C-629/10 *Nelson and Others* [2013] All E.R.

[24] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 49-50.

[25] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 51.

[26] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 52.

[27] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 54 citing, *Liberty and Others v the United Kingdom* [2008] E.C.H.R. 568 at paras 62-63; *Rotaru v Romania* [2000] E.C.H.R. 192 at paras 57-59; and *S. and Marper v the United Kingdom* [2008] E.C.H.R. 1581 at para 99. According to the Court, there is an increased requirement for safeguards where the retained data is subject to automatic processing and there is a significant risk of unlawful access. Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 55.

[28] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 57-58. The Court also criticised the fact that no provision was made in the Directive for obligations of professional secrecy.

[29] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 59.

retention is no longer possible".[30] Following this crucial statement chastising the simple retention of data, the CJEU went on to censure the failure of the Directive to provide sufficient criteria regarding access to the retained data by the competent national authorities.[31]

Accessing retained data can constitute an additional, separate, interference with the privacy rights of an individual. The CJEU criticised the Directive for failing to provide precise rules for accessing the retained data and for providing too much discretion to Member States to "define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data".[32] Of particular concern was the fact that the Directive provided no objective criterion by which the number of persons authorised to access the retained data could be limited.[33] In line with this, the CJEU also criticised the Directive for not mandating independent prior review[34] before access to retained data could be permitted.[35]

In addition to allowing this wide discretion, the Data Retention Directive also provided Member States with significant flexibility on other important issues.[36] The Directive did not provide a concrete definition of what either a "serious crime" or a provider of a "publicly available electronic communications services or of a public communications network" entails.[37] Additionally, the Directive permitted Member States to adopt maximum retention periods of between six and 24 months without regard to whether or not such periods were strictly necessary based on objective criteria.[38] The Directive was censured for the weakness of its provisions

---

[30] The German Civil Liberties group that obtained the documents, AK Vorrat, has stated that "The EU's lawyers have confirmed that a reenactment of a blanket Data Retention Directive - which is under consideration by the EU Commission and would be welcomed by many Member State governments - is no longer a legal option." —, "EU Lawyers Tell Member States: Blanket Communications Data Retention 'No Longer Possible'" *Stoppt Die Vorratsdatenspeicherung!* June 23, 2014. Available at www.vorratsdatenspeicherung.de/content/view/745/1/lang,en/; —, "EU-Juristen halten Vorratsdatenspeicherung wohl für abgehakt" *Heise*, June 23, 2014. Available at www.heise.de/newsticker/meldung/EU-Juristen-halten-Vorratsdatenspeicherung-wohl-fuer-abgehakt-2236498.html; Moody, "EU Lawyers Confirm 'General And Blanket Data Retention Is No Longer Possible' in European Union" *Techdirt*, August 12, 2014. Available at https://www.techdirt.com/articles/20140811/07430928173/eu-lawyers-confirm-general-blanket-data-retention-is-no-longer-possible-european-union.shtml.

[31] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 60-62.

[32] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 60-62.

[33] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 62.

[34] Either by a court or other independent body.

[35] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 62.

[36] Kosta and Valcke "Retaining the Data Retention Directive" (2006) 2 C.L.S.R. 370 at 380.

[37] Article 1(1) of the Directive states that the Directive aims to "harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." Kosta and Valcke "Retaining the Data Retention Directive" (2006) 2 C.L.S.R. 370 at 380.

[38] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 64. In addition to making provision for an extension of the maximum retention period. Kosta and Valcke "Retaining the Data Retention Directive" (2006) 2 C.L.S.R. 370 at 380. In 2011, the European Commission reported that Poland specified a two-year retention period for both types of data and Latvia specified 1.5 years for both types of data. Ten countries – including the United Kingdom – specified one year for both types of data. Cyprus, Luxembourg, and Lithuania specified six months for both data types. Five Member States specified different retention periods for different categories of data. Ireland and Italy specified two years for telephone data and one year for internet data; Slovenia specified 14 months for telephony data and eight months for internet data; Slovakia specified one year for telephone data and six months for internet data; Malta specified one year for telephone data, and six months for internet data. Hungary retained both categories for one year, but only retained data on unsuccessful call attempts for six months. Belgium had specified retention periods of between 12 and 36 months for

regarding the security of retained data[39] and for not requiring that retained data be destroyed following the expiration of the data retention period.[40]

While the CJEU clearly found the Directive to be invalid for failing to comply with the principle of proportionality, the implications of the ruling for each Member State may vary depending on how the Member State has chosen to implement the Directive.[41] The decision itself is also, of course, open to interpretation and whether a Member State adopts a narrow or broad reading of the decision will influence subsequent review of data retention practices. In spite of differences in domestic implementation and interpretation, it is important to monitor responses of other Member States to the CJEU ruling. In addition to highlighting the more significant implications of the CJEU ruling, examining the responses of other Member States can provide useful insight when addressing the question of how the law may develop in Ireland.

Responses of Members States

The Data Retention Directive has been controversial since its inception,[42] and the domestic courts of several Member States have found aspects of the Directive to be unconstitutional. In a steady stream of decisions, the Bulgarian Supreme Administrative Court, the Romanian Supreme Court, and the German Constitutional Court found the Directive unconstitutional in 2008, 2009, and 2010 respectively. These decisions were followed by the Czech Constitutional Court and the Cyprus Supreme Court, which both found the Directive to be unconstitutional in 2011.[43] As the genesis of the decision of the CJEU came from a preliminary reference from the Irish High Court, the decision has immediate repercussions for the Irish system. The *Digital Rights Ireland* case will resume at the domestic level and the High Court will consider whether the Irish law on data retention – The Communications (Retention of Data) Act 2011 – is unconstitutional. McIntyre has pointed out that

> "It is difficult to see how the national law implementing the Directive can stand up to challenge now that the Directive itself has been held invalid. Consequently it is very likely that new Irish legislation will be proposed."[44]

As we wait to see how the High Court – and the Government – responds to the decision of the CJEU, it is worth considering how other Member States have responded to the ruling. While the Opinion of the Advocate General in *Digital Rights Ireland* also found the Data Retention Directive

---

"publically available" telephone services and had not specified retention periods for internet data. Report From The Commission To The Council And The European Parliament Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (April 18, 2011) COM(2011) 225 at 13-14.

[39] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 67.

[40] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 67.

[41] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 69.

[42] Ireland had previously challenged the legal basis of the Directive, but the CJEU found the legal basis to be appropriate under EU law. *Ireland v European Parliament* [2009] E.C.R. I-593. From its inception the European Data Protection Commissioners have expressed grave doubts about data retention and in 2002 argued that the "systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case". Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9–11 September 2002) on mandatory systematic retention of telecommunication traffic data (September 9, 2002). Available at http://www.datenschutz-berlin.de/doc/eu/konf/02_manda_sys.htm; Kosta and Valcke "Retaining the Data Retention Directive" (2006) 2 C.L.S.R. 370 at 371.

[43] Kosta, "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection (2013) 10 *SCRIPTed* 340 at 340.

[44] McIntyre, "Surveillance judgment is a victory for democracy" *Irish Independent*, April 10, 2014. Available at www.independent.ie/opinion/analysis/surveillance-judgment-is-a-victory-for-democracy-30172786.html

to be incompatible with the Charter, the Advocate General recommended that the effects of any finding against the Directive should be suspended until the legislative branches of the EU had the opportunity to introduce corrective legislation.[45] The CJEU provided no such latitude, however, and the European Commission promptly released a statement clarifying that domestic legislation that was contrary to EU law following the ruling of CJEU would need to be amended.[46]

Due to the strength of the CJEU ruling, domestic data retention measures will require significant scrutiny across the EU. The preliminary reference made by the Irish High Court regarding the validity of the Data Retention Directive was joined by a similar reference from an Austrian Court. Since the *Digital Rights Ireland* decision, the Austrian Constitutional Court found parts of the domestic data retention law to be in breach of the fundamental right to data protection and the right to respect for private life as guaranteed under Article 8 of the European Convention on Human Rights.[47] In line with the decision of the Austrian Constitutional Court, the Slovenian Constitutional Court has also found the domestic rules on data retention to be invalid. Echoing the decision of the CJEU, the Slovenian Constitutional Court criticised the disproportionate retention of data of a large proportion of the population without providing reasonable justification for the mass retention.[48] In addition, the Romanian Constitutional Court has found the Romanian data retention regime to be unconstitutional,[49] and the Slovakian Constitutional Court has issued a preliminary suspension of domestic data retention while a challenge to the regime is pending.[50]

While these recent developments suggest a strong trend in favour of increased proportionality and in opposition to blanket surveillance, not all Member States have responded to the ruling of the CJEU in a similarly privacy-positive manner. Both Sweden and Denmark maintain the legality of their current data retention regimes and highlight the differences between their domestic regimes and the Data Retention Directive in order to distinguish their national laws from the condemned Directive.[51] While the positions taken by authorities in Sweden and Denmark can be criticised for adopting conveniently narrow interpretations of the decision of

---

[45] Advocate-General Opinion in Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] E.U.E.C.J. at paras 154-158.

[46] European Commission, "Frequently Asked Questions: The Data Retention Directive" *Press Release.* Available at europa.eu/rapid/press-release_MEMO-14-269_en.htm.

[47] Press Release, "Austrian Laws on Data Retention Found Unconstitutional" *Verfassungerichtshof Osterreich*. Available at www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/press_releasedataretention.pdf.

[48] Press Release, "Slovenian Constitutional Court holds data retention unconstitutional, orders deletion of data Information Commissioner". Available at https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461; Digital Rights Ireland, "Data retention held unconstitutional in Slovenia" *Digital Rights Ireland* July 12, 2014. Available at www.digitalrights.ie/data-retention-slovenia-unconstitutional/.

[49] Digital Rights Ireland, "Romanian Constitutional Court holds data retention unconstitutional" *Digital Rights Ireland* July 9, 2014. Available at http://www.digitalrights.ie/romanian-constitutional-court-holds-data-retention-unconstitutional/.

[50] E.I.S.I., "Slovak Constitutional Court Suspends Data Retention Legislation" *E.I.S.I.*, April 24, 2014. Available at www.eisionline.org/index.php/projekty-m/ochrana-sukromia/74-us-data-retention-suspension

[51] The Swedish Ministry of Justice has issued a preliminary assessment concluding that Swedish rules are lawful as Swedish domestic legislation provides for clear rules regarding access to the retained information. A report commissioned by the Danish Parliament concluded that Danish system met the proportionality requirements as described in the Digital Rights Ireland decision. Press Release, "Swedish law manages the EU's requirements for data storage" *Regeringskansliet*. Available at www.regeringen.se/sb/d/18730/a/242377; See Genna, "The Data Retention Tsunami: How EU Member States are Reacting to the Annulment of the Data Retention Directive" *Radio Bruxelles Libera*, June 27, 2014. Available at radiobruxelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/radiobruxelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/.

the CJEU,[52] from the Irish perspective, the actions of our closest neighbour, the United Kingdom, call for closest attention at this point.

The UK Government has been a staunch advocate for data retention, arguing that it is essential in order to "identify suspects, examine their contacts, establish relationships between conspirators, and place them in a specific location at a certain time" and to "draw up a detailed profile of the suspect(s) either to inform prevention/disruption operations or for use as corroborative evidence in a prosecution".[53] The UK Government has gone as far to say that data retention can mean "the difference between life and death".[54] Unlike Ireland, the United Kingdom did not introduce a domestic law based on the Data Retention Directive. Instead, the United Kingdom relied on a ministerial order that transposed the Directive into UK law directly.[55] Accordingly, following the decision of the CJEU in *Digital Rights Ireland*, the United Kingdom confronted a pressing problem as the legal basis for its data retention policy had been entirely undermined.[56]

In a decision that has been viewed by many as strategic, the UK government introduced the Data Retention and Investigatory Powers Act 2014 (DRIPA) as an emergency piece of legislation in July 2014. According to the UK Home Secretary, Theresa May, the new legislation was necessary to address the fact that the ruling of the CJEU in *Digital Rights Ireland* put the legal basis for UK data retention into question. In spite of the fact that May characterised the legislation as essential to counteract the legal ambiguity that arose following the CJEU ruling in April, plans to introduce the legislation were not revealed until 10 July 2014, three months after the CJEU ruling. In response to the decision to introduce the new law as emergency legislation, David Davis pointed out that the claimed emergency was a "predictable" one.[57] While the Bill was only published on 10 July 2014, the Bill received the royal assent just seven days later. Accordingly, the government has been criticised for avoiding parliamentary scrutiny and public debate.[58] Shadow Home Secretary, Yvette Cooper admonished the timing of the legislative proposal and the short period provided to members of Parliament to consider the legislation before voting.[59]

---

[52] Järvinen, "Denmark: Data retention is here to stay despite the CJEU ruling" *E.D.R.I.*, June 4, 2014 . Available at edri.org/denmark-data-retention-stay-despite-cjeu-ruling/; See Genna, "The Data Retention Tsunami: How EU Member States are Reacting to the Annulment of the Data Retention Directive" *Radio Bruxelles Libera*, June 27, 2014. Available at radiobruxelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/radiobruxelleslibera.wordpress.com/2014/06/27/data-retention-down-in-austria/.

[53] Home Office Consultation, "Access to communications data – respecting privacy and protecting the public from harm" (March 27, 2003); Walker, "Data retention in the UK: Pragmatic and Proportionate, or a Step Too Far? (2009) 25 C.L.S. Rev. 325 at 325.

[54] Home Office, *Protecting the Public in a Changing Communications Environment* (The Stationery Office, 2009) at 1; Walker, "Data retention in the UK: Pragmatic and Proportionate, or a Step Too Far? (2009) 25 C.L.S. Rev. 325 at 325.

[55] The Data Retention (EC Directive) Regulations 2007. Available at www.legislation.gov.uk/uksi/2007/2199/contents/made; The Data Retention (EC Directive) Regulations 2009. Available at www.legislation.gov.uk/uksi/2009/859/contents/made.

[56] Lillington, "UK Data law is good news for Ireland's tech sector" *Irish Times*, July 17, 2014. Available at http://www.irishtimes.com/business/sectors/technology/uk-data-law-is-good-news-for-ireland-s-tech-sector-1.1868579.

[57] Mason, "MPs Raise Fears Over Move To Push Surveillance Bill Through Commons" *The Guardian*, July 10, 2014. Available at www.theguardian.com/politics/2014/jul/10/ministers-emergency-surveillance-law-push-commons.

[58] Watson, "Forcing Through the Surveillance Laws is a Further Erosion of Political Trust" *The Guardian*, July 10, 2014. Available at www.theguardian.com/commentisfree/2014/jul/10/forcing-through-surveillance-laws-erosion-political-trust.

[59] HC Deb 10 July 2014 col 459.

The government used the emergency legislative procedure and the threat of terrorism and paedophilia to rush through legislation without significant review. In the House of Commons, May stated that the legislation was necessary to prevent criminals from escaping justice.[60] Similarly, the Prime Minister, David Cameron, relied heavily on the perceived security benefits of data retention in his defence of the law. Cameron argued that in today's "dangerous world" it is sometimes necessary to "listen to someone's phone and read their emails to identify and disrupt a terrorist plot". According to Cameron, the new law was necessary in order to maintain existing capabilities that are "vital" to national security and necessary to "to keep our country safe". He alluded to a diverse range of threats from paedophiles to the "growth of Isis in Iraq".[61]

The Government also downplayed the significance of DRIPA by asserting that the new law was designed "to strengthen and clarify, rather than extend, the current legislative framework" and that the law did not provide for any "additional investigatory powers".[62] Even though the government characterised the Act as clarifying the status quo, many commentators, including a coalition of specialist academics, have argued that the new legislation actually extends the scope of the current data retention regime by expanding the definition of "telecommunications service" and including new jurisdictional powers to compel companies operating abroad to comply with UK orders.[63] The false characterisation of the law appears to be an additional tactic to get the law enacted with the minimum amount of scrutiny.

Putting the claims of expansion aside, examination of the DRIPA reveals that the legislation introduced in response to the decision in *Digital Rights Ireland* does very little to respond to the fundamental rights concerns expressed by the CJEU.[64] When justifying the UK retention regime as proportionate, Theresa May focused almost entirely on the safeguards built into the Regulation of Investigatory Powers Act 2000 (RIPA).[65] RIPA only governs access to data and a key aspect of the CJEU ruling criticised the blanket retention of data.[66] Accordingly, the protections provided by RIPA do nothing to address an important section of the *Digital Rights Ireland* ruling. The UK government also attempted to assert that DRIPA had enhanced the proportionality of the retention policy by modifying the mandatory data retention period of 12 months to a *maximum* data retention period of 12 months.[67] While this would in theory allow for

---

[60] Wintour, Mason and Ball, "David Cameron Makes Concessions to Rush Through Snooping Law" *The Guardian*, July 10, 2014. Available at www.theguardian.com/world/2014/jul/10/david-cameron-concessions-snooping-law-surveillance.

[61] Wintour, "Surveillance law wins cross-party support but critics claim stitch-up*" The Guardian*, July 10, 2014. Available at www.theguardian.com/world/2014/jul/10/surveillance-legislation-commons-support-critics-stitch-up.

[62] Explanatory Notes, Data Retention And Investigatory Powers Bill 2014 (July 15, 2014). Available at www.publications.parliament.uk/pa/bills/lbill/2014-2015/0037/en/15037en.htm.

[63] An open letter from UK internet law academic experts to all Members of Parliament (July 15, 2014). Available at paulbernal.wordpress.com/2014/07/15/open-letter-from-uk-legal-academic-experts-re-drip/; For analysis of the new law see Smith, "Mandatory communications data retention lives on in the UK - or does it?" *Bird & Bird*, July 22, 2014. Available at www.twobirds.com/en/news/articles/2014/uk/mandatory-communications-data-retention-lives-on-in-the-uk; Smith, "Dissecting DRIP - The Emergency Data Retention and Investigatory Powers Bill" *Cyberleagle*, July 12, 2014. Available at cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html.

[64] Hickman, "Tom Hickman on the DRIP Bill: Plugging Gaps in Surveillance Laws or Authorising the Unlawful?" *U.K. Const. L. Blog*, July 14, 2014. Available at ukconstitutionallaw.org/2014/07/14/tom-hickman-on-the-drip-bill-plugging-gaps-in-surveillance-laws-or-authorising-the-unlawful/.

[65] Home Office and The Rt Hon Theresa May MP Oral statement to Parliament Communications data and interception (July 10, 2014). Available at https://www.gov.uk/government/speeches/communications-data-and-interception.

[66] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 para. 59.

[67] Theresa May argued that this measure addressed the proportionality issue by introducing "differentiation" and allowing for retention notices issued to Communications Service Providers to be applicable for a shorter period of time if a shorter period is "felt to be right" by the Secretary of State. HC Deb 15 July 2014 col 711.

more proportionate retention, DRIPA provides no protection against the Secretary of State simply deciding that a 12 month period of retention is necessary in every case.[68] The fact that DRIPA requires the Secretary of State to only mandate retention where he or she considers the retention to be necessary and proportionate pays only symbolic lip-service to the issues raised in *Digital Rights Ireland*.

Ireland and data retention

In spite of original objections to the legal basis for the Data Retention Directive, Ireland has been a strong supporter of data retention law at the EU level.[69] Even though the CJEU found that the Data Retention Directive constituted a serious interference with fundamental rights, the fact that the CJEU found that the Directive did not interfere with the "essence" of those rights is a source of support for proponents of data retention.[70] In spite of this, it is clear from the *Digital Rights Ireland* ruling that data retention is only permissible where appropriate safeguards are in place in order to ensure that retention measures are strictly necessary in the fight against serious crime. Under Article 52 of the EU Charter, rights may only be limited if the limitations are necessary and genuinely meet objectives.[71] In order to be proportionate, limitations on rights must be "appropriate for attaining the legitimate objectives pursued" and must not "exceed the limits of what is appropriate and necessary in order to achieve those objectives".[72]

In order to ensure compliance with the EU Charter, it is essential that the Irish legislature rejects the UK approach and engages in a genuine evaluation of the CJEU opinion. The Communications (Retention of Data) Act 2011 is the governing law on data retention in Ireland and it appears that the Irish government is adopting a "wait-and-see" approach in anticipation of the *Digital Rights Ireland* case returning to the High Court. The Minister for Justice, Frances Fitzgerald, has stated that legal advisors to the government have indicated that the Communications (Retention of Data) Act 2011 stands in the absence of any High Court ruling to the contrary.[73] Regardless of the outcome in the High Court, the importance of the CJEU ruling necessitates a thorough examination of the Irish regime.

As it is a challenge to find a less intrusive measure that achieves the same objective as data retention, it is especially important to consider what limitations will enable proportionate data retention. Currently, the Communications (Retention of Data) Act 2011 obliges service providers to retain telephony data for two years and internet data for 12 months.[74] The Act compels service providers to comply with disclosure requests made by An Garda Síochána, the Defence Forces, and the Revenue Commissioners.[75] Utilising the discretion granted by the Data Retention Directive, the Communications (Retention of Data) Act 2011 defines a "serious offence" as an

[68] It is important to note that the Secretary of State can issue a notice requiring a certain period of data retention to a description of operators and not just a single operator.
[69] T McIntyre, "Data Retention in Ireland: Privacy, Policy and Proportionality" (2008) 24 C.L.S.R 326 at 326-330. Some commentators have speculated that the motivation behind support for EU regulation was reduced political scrutiny. K Lillington, "Back door policy for data retention wrong" *Irish Times*, July 30, 2004.
[70] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 39-40.
[71] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 38.
[72] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 46.
[73] Joint Oireachtas Committee on Justice, Defence and Equality Justice and Home Affairs Council, *Discussion* June 25, 2014.
[74] Communications (Retention of Data) Act 2011 s. 3.
[75] Communications (Retention of Data) Act 2011 ss. 6-7.

offence "punishable by imprisonment for a term of 5 years or more".[76] Depending on the agency involved, disclosure requests may be made by a member of an Garda Síochána not below the rank of chief superintendent,[77] a Colonel in the Permanent Defence Forces,[78] or an Officer of the Revenue Commissioners of at least principal officer rank.[79]

If data retention is to continue in Ireland, it is recommended that greater proportionality could be introduced to the process in a number of key ways. It will be necessary in the first instance to reduce the enormous scope of current retention. The current practice of retaining all communications, regardless of any connection to serious crime, is unjustifiable from the point of view of the proportionality principle. Retention of the communications of individuals who are suspected of criminal activity has merit and provision should be made for the targeted retention of the communications of suspected individuals. As retention can only be justified where it is necessary in the investigation of serious crime, the scope of the domestic definition of serious crime could have serious implications for the proportionality of a retention regime. While the Communications (Retention of Data) Act 2011 does provide detail regarding what crimes are considered to constitute serious offences, a review of current practice should also include an appraisal of whether the current definition only includes crimes which are sufficiently serious in order to justify the intrusion.[80]

New legislation should also address the fact that the mandated retention periods of 12 and 24 months in the Communications (Retention of Data) Act 2011 do not account for proportionality. Evidence suggests that the vast majority of retained data used by investigative authorities is six months old or less.[81] According to a report of the EU Commission, information provided by Member States suggested that around 70% of data accessed by investigative authorities is actually just three months old or less.[82] By limiting data retention to a *maximum* period of six months, and requiring the destruction of the retained data on the expiry of that time period, the extent of the privacy interference would be significantly reduced but the benefits of retention would remain largely intact. Under the EU Directive on Privacy and Electronic

---

[76] In addition, provision was made for a number of additional offenses to be included under the definition of serious offence. Schedule 1 lists the following as additional crimes that come under the definition of "serious offence": 1. An offence under sections 11 and 12 of the Criminal Assets Bureau Act 1996; 2. An offence under section 6 of the Criminal Evidence Act 1992; 3. An offence under section 12 of the Non-Fatal Offences against the Person Act 1997; 4. An offence under section 1 of the Prevention of Corruption Acts 1889 to 1995; 5. An offence under section 5 of the Protections for Persons Reporting Child Abuse Act 1998.

[77] The disclosure request must be for the purpose of the prevention, detection, investigation and prosecution of serious crime, safeguarding the security of the State and saving human life. Communications (Retention of Data) Act 2011 ss. 6-7; —, "Data Retention: Telecoms and Internet" [2011] Ann. Rev. Irish L. 116 at 124-125.

[78] The disclosure request must be for the purpose of safeguarding the security of the State. Communications (Retention of Data) Act 2011 s. 6; —, "Data Retention: Telecoms and Internet" [2011] Ann. Rev. Irish L. 116 at 124-125.

[79] The disclosure request must be for the investigation of a "serious offence" under one of the following pieces of legislation: section 186 of the Customs Consolidation Act 1876; section 1078 of the Taxes Consolidation Act 1997; section 102 of the Finance Act 1999; section 119 of the Finance Act 2001; section 79 (inserted by section 62 of the Finance Act 2005) of the Finance Act 2003; section 78 of the Finance Act 2005. Communications (Retention of Data) Act 2011 s. 6.

[80] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at paras 60-61. Of particular focus here may be the entitlement of the Revenue Commissioner to seek data in the investigation of certain financial crimes.

[81] A 2011 Report by the EU Commission stated that quantitative data submitted by Member States suggested that around 90% percent of the data accessed by investigative authorities was six months old or less. Report From The Commission To The Council And The European Parliament Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (April 18, 2011) COM(2011) 225 at 15.

[82] Report From The Commission To The Council And The European Parliament Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (April 18, 2011) COM(2011) 225 at 15.

Communications, data may be stored for a limited period where the retention is proportionate and necessary in order to protect national security or to investigate crime.[83] This was interpreted for data protection purposes as requiring that data be retained for a maximum of six months.[84] When presenting the Communications (Retention of Data) Bill to the Seanad, however, Deputy Michael Finneran stated that the limitation of the retention period to six months had

> "left this country with a dilemma, as clearly the law enforcement authorities required data to be retained for longer than six months if they were not to be severely handicapped in their ability to fight crime and safeguard State security".[85]

The evidence for this purported handicap was limited. In fact, Finneran admitted that "most retained data that is required is requested by those authorities within six months of it being generated or processed". In spite of this, the Deputy went on to assert that the retention of data for "longer periods can be equally important in fighting crime, including terrorist crime."[86] The natural conclusion of such a thought process is that longer periods should be permitted in all situations, regardless of any proportionality analysis or consideration of rights, just as long as the information could potentially be useful.[87] A different approach – that makes provision for the use of expanded retention periods, while also respecting the principle of proportionality – is the use of a "quick-freeze" procedure.[88] This term is used to describe the emergency retention of data for an extended period where it is believed that the data may be crucial for the investigation of a crime. An Garda Síochána could, for example, request that data connected with certain individuals,[89] locations, or temporalities could be retained while police continue to conduct

[83] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] O.J. L-201 art. 15.

[84] This was the opinion of the Data Protection Commissioner. See Meade, "Retention of Communications Traffic Data" *Press Release Data Protection Commissioner*, February 24, 2003. Available at https://www.dataprotection.ie/Viewtxt.asp?DocID=224; Report Of The Minister For Communications, Marine & Natural Resources On The Public Consultation Process On The Transposition Into Irish Law Of EU Directive 2002/58/EC Concerning Data Protection And Privacy In Electronic Communications (July, 2004) at 5. Available at http://www.dcenr.gov.ie/NR/rdonlyres/945A2714-37D0-4FE3-AC65-5D84EDF34DF1/0/Comms_Reg_Data_Protection_Report_on_Public_Consultation.doc. Seanad Deb 29 April, vol 202(6), col 391-395.

[85] Seanad Deb 29 April, vol 202(6), col 391-395.

[86] Seanad Deb 29 April, vol 202(6), col 391-395.

[87] Seanad Deb 29 April, vol 202(6), col 391-395; —, "Data Retention: Telecoms and Internet" [2011] Ann. Rev. Irish L. 116 at 119-120.

[88] See Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC [2005] O.J. C-298.
. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf; Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp64_en.pdf.

[89] This could be useful where, for example, the police suspect that an individual may be involved in a crime but they do not have a sufficient amount of proof to justify accessing the individual's communication data. A quick-freeze procedure would allow that individual's information to be retained in the event that more evidence arises at a later date. See Bignami, "Privacy and Law Enforcement in the European Union: The Data Retention Directive" (2007) 8 Chi. J.I.L. 233 at 249.

investigations. Such an approach avoids mass surveillance, but takes the investigative benefits of retention into account.[90]

In addition to reducing the sheer amount of data being retained, a compliant data retention regime must also contain protections ensuring the proportionate access to the retained data. The safeguards provided by the Irish Act are so minimal as to hardly address the concerns expressed by the CJEU in *Digital Rights Ireland*. A significant failure of the Communications (Retention of Data) Act 2011 is the ability of a member of the executive branch – a senior officer in either an Garda Síochána, the Defence Forces, or the Revenue Commission – to make disclosure requests in the absence of any judicial involvement. It was clear from the judgment of the CJEU that some independent authorisation is necessary in order to ensure that access will only be granted where it is strictly necessary.[91] The involvement of an independent authorising body would also assist in the goal of limiting the number of people who have access to retained data.[92] Experience has shown that the provision for limited and post hoc judicial review in the Communications (Retention of Data) Act 2011 is an ineffective and insufficient safeguard.[93] In any case, it is also that "[r]etrospective review is likely to be less rigorous than prior scrutiny and it may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance".[94] The Criminal Justice (Surveillance) Act 2009 requires authorisation from a District Court judge for the use of surveillance devices in Irish law.[95] To protect operational security, proceedings under the Criminal Justice (Surveillance) Act 2009 are held ex parte and in camera. Accordingly, there is no practical reason why a judicial body cannot play a similar role in granting access to retained data.[96]

Conclusion

While the Australian government may point to DRIPA for support when defending its proposed Data Retention regime and assert that increased data retention is an inevitability in modern society,[97] the ruling in *Digital Rights Ireland* – in addition to congruent decisions in several domestic courts across the EU – demonstrates significant push back against the tide of mass surveillance. If Ireland is to be in compliance with its fundamental rights obligations, it is imperative that the government engages in a genuine appraisal of the current system and rejects the rushed and superficial approach that the UK government adopted when introducing DRIPA. The principle of proportionality must be the central focus of reform efforts in order to find the

[90] The quick-freeze procedure directly responds to the CJEU criticism of blanket retention policies which do not attempt to restrict retention based on time periods, geographical zones, or circles of people. Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 59.
[91] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 62.
[92] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] W.L.R.(D) 164 at para. 62
[93] The strength of the Designated Judge as a safeguard has been criticised, including in debates of the Oireachtas and in the media. Seanad Deb 5 May, vol 136, col 480; Tighe, "Judges' Phone Tap Report 'is laughable'" *Sunday Times*, May 23, 2009. Available at http://www.timesonline.co.uk/tol/news/world/ireland/article6350866.ece. Gillespie, "Covert Surveillance, Human Rights and the Law" (2009) 3 I.C.L.J. 71 at 74; Murphy, "The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases" (2013) 3 I.J.L.S. 65 at 83.
[94] Ferguson and Wadham, "Privacy and Surveillance: A Review of the Regulation of the Investigatory Powers Act 2000" [2003] E.H.R.L.R. 101 at 105.
[95] Criminal Justice (Surveillance) Act 2009 ss. 4-5.
[96] Criminal Justice (Surveillance) Act 2009 ss. 4-5.
[97] G Moody, "Australia's Attorney-General: Data Retention Is 'Very Much The Way In Which Western Nations Are Going'" *Techdirt*, July 17, 2014. Available at https://www.techdirt.com/articles/20140716/05151827888/australias-attorney-general-data-retention-is-very-much-way-which-western-nations-are-going.shtml; Taylor, "Data retention is 'the way western nations are going': Brandis" *ZD Net*, July 16, 2014. Available at www.zdnet.com/au/data-retention-is-the-way-western-nations-are-going-brandis-7000031658/.

appropriate balance between the "interests of the individual and the interest of the wider community."[98]

When accounting for proportionality at the legislative level, it is clear there is an abstract element to the concept. Accordingly, it is logical to require safeguards that act to ensure that the exercise of power is under control and subject to review. The application of the proportionality principle must be genuine and the legislature must be alert to avoid empty assertions of proportionality without supporting those claims with appropriate safeguards and mechanisms. The terse assurances of proportionality in DRIPA and associated government documents illustrate the risk that such an approach poses to the protection of fundamental rights.[99]

When proposing data retention reforms, the Irish government should explicitly justify its policy choices by reference to the principle of proportionality. In order to determine what is proportionate, the government should not shy away from the foundational questions, such as how effective data retention is in the investigation of serious crime.[100] The role any safeguards are claimed to play in the enhancement of proportionality should be supported by the government with fully reasoned arguments and evidence. Such an approach would enhance transparency and discourage disingenuous assertions of proportionality such as those made by UK Government when discussing DRIPA.[101] DRIPA serves as a warning; the Irish government should resist the temptation to circumvent challenge and should embrace full and informed public debate.

[98] Taylor, "Policing Privacy and Proportionality" [2003] E.H.R.L.R. 86 at 88.
[99] Powles, "UK's DRIP law: Cynical, Misleading and an Affront to Democracy" *The Guardian*, July 18, 2014. Available at www.theguardian.com/technology/2014/jul/18/uk-drip-ripa-law-sceptical-misleading-democracy-martha-lane-fox.
[100] While the Irish and Austrian governments presented statistics to the CJEU in *Digital Rights Ireland* ostensibly in support of the effectiveness of data retention, there remains a lack of scientific support for the mass retention of data; Jones and Hayes, "The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy" (2013) *SECILE* at 32. Available at secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf; Emert, "Data Retention might not be Proportional to Risks" *Internet Policy Review*, July 9, 2013. Available at http://policyreview.info/articles/news/data-retention-might-not-be-proportional-risks/170; Lillington, "State Agencies Target Irish Phone and Internet Records" *The Irish Times*, July 25, 2013.
[101] See generally, HC Deb, 15 July 2014.