[2018] IEHC 685

THE HIGH COURT

[2015 No. 351 P]

BETWEEN

GRAHAM DWYER

PLAINTIFF

AND

COMMISSIONER OF AN GARDA SÍOCHÁNA, MINISTER FOR COMMUNICATIONS, ENERGY AND NATURAL RESOURCES, IRELAND AND ATTORNEY GENERAL

DEFENDANTS

JUDGMENT of Mr. Justice Tony O'Connor delivered the 6th day of December, 2018

TABLE OF CONTENTS

1. INTRODUCTION

1.1 In what circumstances does a democracy tolerate State mandated electronic surveillance of every citizen who uses a telephone device? To what extent is the State bound by European Union law (**"EU law"**) and the European Convention on Human Rights (**"ECHR"**) when introducing or applying domestic law which provides for mass electronic surveillance? What effect have the "*dispositifs*" (judgments by way of communications from the European Court of Justice (**"ECJ"**)) on Courts of other Member States on applying EU law in Ireland?

1.2 Can An Garda Síochána (**"Gardaí"**) implement the generally stated purpose of legislation enacted under the Constitution without specific statutory protections for the fundamental right of privacy in the legislation? How appropriate, necessary and proportionate is a law that requires all providers of electronic communications services (**"service providers"**) to gather and store information which is not otherwise collected? Are precautions required to guarantee democratic principles when intruding on privacy rights? Do deterrence, investigation and prosecution for murder and other serious offences, which are a clear threat to society, justify a total or partial relaxation of safeguards? How is the purpose of legislation interpreted and applied when retaining or accessing data? Does one enquire about:-

(i) the justification for gathering, retention and access; and

(ii) the device user (whether parliamentarian, journalist, doctor, lawyer or whoever).

1.3 Do murder and other abhorrent crimes which transgress the fundamental rules for an orderly society permit the State to legislate for general and indiscriminate surveillance? Does it matter if the State contends or establishes that alternatives (such as surveillance targeted on groups, areas or time), will not assist the detection of particular serious crimes and will undermine investigations and prosecutions?

1.4 What remedy is available to a citizen whose privacy is infringed by a breach of law? Can the remedy be limited, i.e. be applied prospectively or suspended?

1.5 The above are questions which are touched upon in this judgment. It is lengthy not least because the context for the above questions include some detail about the investigation leading to the conviction of the Plaintiff for the murder of Ms. Elaine O'Hara in 2012. Recent developments in the law concerning the issues now before this Court also call for consideration.

Questions posed by the Plaintiff

1.6 The specific questions posed by the Plaintiff in his claim relate to whether provisions of the Communications (Retention of Data) Act 2011 (**"2011 Act"**), that authorise general retention and then access of specific data, are incompatible with:-

(i) Article 5(4) of the Treaty of the European Union (**"TEU"**) which applies "*the principle of proportionality*" to actions of the Union;

(ii) Articles 7 (respect of private and family life), 8 (protection of personal data), 11 (freedom of expression and information), 41 (right to good administration), 52 (limitation of rights must be provided by law) of the Charter of Fundamental Rights of the European Union (**"Charter"**);

(iii) Article 8 (right to respect for private and family life) and Article 10 (freedom of expression) of the ECHR.[i]

This part of the claim is in addition to the plea that provisions of the 2011 Act are repugnant to the Constitution having regard to the duty of the State under Article 40.3.1˚ (to vindicate personal rights), 40.3.2˚ (protect from unjust attack) and 40.6.1˚ (liberty to exercise right of expression).

Main EU legislation and cases

1.7 The following are the relevant EU directives:

(i) 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, O.J. L281/31 23.11.1995 (**"1995 Directive"**);

(ii) 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, O.J. L201/37 31.7.2002 (**"2002 Directive"**);

(iii) 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 communication services or of public communications networks and amending Directive 2002/58/EC, L105/54 13.4.2006 (**"2006 Directive"**).

1.8 The judgments of the Court of Justice (**"ECJ"**), which, along with the General Court, make up the Court of Justice of the European Union (**"CJEU"**), in:

(i) *Ireland v. Parliament and Council (Case C-301/06)* [2009] E.C.R. I-593 (***"Ireland v. Parliament"***);

(ii) *Digital Rights Ireland Limited v. Minister for Communications, Marine and Natural Resources & Ors* and *Kärntner Landesregierung and Others (Joined Cases C-293/12 and C-594/12)* [ECLI:EU:C:2014:238] (***"Digital Rights"***); and

(iii) *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others (Joined Cases C-203/15 and C-698/15)* [ECLI:EU:C:2016:970] (***"Tele2"***).

are to the forefront of the tussle between the parties.

2011 Act

Retention

1.9 Section 3(1) requires all service providers to retain, *inter alia*, data described in Schedule 2 Part 1, limited for two years. This is categorised as fixed network telephony and mobile telephony data which is described as data to identify the source, destination, timing of start and end, geographic location and type of equipment used (**"telephony data"**). Section 1 also defines the data as "*traffic data or location data and the related data necessary to identify the subscriber or user*." Content of communications do not fall within the definition of telephony data.

Access

1.10 Section 6(1) provides:-

> "*A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for–*
>
> *(a) the prevention, detection, investigation or prosecution of a serious offence,*
>
> *(b) the safeguarding of the security of the State,*
>
> *(c) the saving of human life.*"

1.11 The 2011 Act provides nothing more for access to telephony data by the Gardaí.

1.12 Section 7 obliges a service provider to comply with a disclosure request.

Security of Data

1.13 Sections 4 and 5 restrict service providers in their activities under the 2011 Act in such a way as to protect telephony data under their control.

Complaints and Supervision

1.14 Section 10(1) provides:-

> "*A contravention of section 6 in relation to a disclosure request shall not of itself render that disclosure request invalid or constitute a cause of action at the suit of a person affected by the disclosure request, but any such contravention shall be subject to investigation* [by the Referee, currently a Circuit Court Judge nominated under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (**"1993 Act"**)] *in accordance with the subsequent provisions of this section and nothing in this subsection shall affect a cause of action for the infringement of a constitutional right*".

1.15 Notably, a person affected by a request is not necessarily informed of the request before or after the request is made. This begs the question as to how and when investigations are requested. Section 9 does indeed require the Garda Commissioner to furnish statistics to the Minister with responsibility for the Gardaí and the Defendants infer that this can be tied in with duties of the Data Protection Commissioner (**"DPC"**) who is the nominated supervisory authority under s. 4(2).

1.16 Section 12 requires the designated High Court Judge under the 1993 Act to review and report on the operation of the provisions of the 2011 Act to the Taoiseach. The designated judge may communicate with the Taoiseach or the Minister for Justice, Equality and Law Reform concerning disclosure requests.

Plaintiff's claim

1.17 The claim ultimately comes down to alleging that:-

(i) Section 3(1) of the 2011 Act contravenes Article 15(1) of the 2002 Directive read in light of:

a. Articles 7, 8, 11 and 52(1) of the Charter and

b. Articles 8 and 10 of the ECHR

in so far as it permits the **retention** of telephony data in a manner which is **general and indiscriminate**;

(ii) Section 6(1) and s. 7 of the 2011 Act contravenes Article 15(1) of the 2002 Directive read in light of Articles 7, 8, 11 and 52(1) of the Charter in so far as it permits **the accessing** of the retained telephony data **other than on foot of prior review by a court or an administrative authority**;

(iii) Sections 3, 6 and 7 of the 2011 Act are:

a. incompatible with the obligations of the State under Articles 8 and 10 of the ECHR and

b. repugnant to Articles 40.3.1º, 40.3.2º and 40.6.1º of the Constitution for the same reasons given in respect of the challenge under the Charter.

Excluded from review in this judgment

1.18 In the interests of clarity, this judgment is not concerned with retention or access for "*the safeguarding of the security of the State*" or "*the saving of human life*" which are the two other objectives covered by the 2011 Act (s. 6(1)(b) and (c)). Any reference to s. 6(1) in this judgment refers only to retention for "*the prevention, detection, investigation or prosecution of a serious offence.*" (s. 6(1)(a)).

1.19 Furthermore, the debate before this Court concentrated on mobile telephony data. Therefore, other types of data which are retained whether through private agreements or otherwise do not fall within the remit of the discussion. Data that is defined in Part 2 of Schedule 2 of the 2011 Act and which is retained for one year is not addressed specifically in this judgment.

2. BACKGROUND

The Conviction and Use of Data

2.1 On 27th March, 2015, the Plaintiff was convicted by a jury of the murder of Ms. Elaine O'Hara (**"the Victim"**) for which he received a life sentence on 25th April, 2015. The investigation leading to the trial used the mobile telephony data generated by the phone provided by the Plaintiff's employer to the Plaintiff (**"407 phone"**). This data was retained and accessed under the 2011 Act.

2.2 Counsel for the Plaintiff applied to the trial Judge (Hunt J.) to exclude the telephony data for the 407 phone. Hunt J., following a *voir dire*, ruled that the data could be adduced in evidence. Submissions had been made concerning the operation of the 2011 Act in view of:-

(i) The 2006 Directive;

(ii) The judgment in *Digital Rights* delivered on 8th April, 2014 which declared the 2006 Directive to be invalid; and

(iii) The Charter.

2.3 It had been submitted to Hunt J. in February 2015, that the alleged breach of the Charter should be approached by applying the test adopted by the majority of the Supreme Court in *DPP v. Kenny* [1990] 2 I.R. 110 (**"*DPP v. Kenny*"**). The law established in this case changed after the criminal trial of the Plaintiff as a result of the majority judgments of the Supreme Court in *DPP v. J.C.* [2017] 1 I. R. 417, delivered on 15th April, 2015, (**"*J.C.*"**). This Court does not concern itself with the ruling of Hunt J. or the admission of evidence. The conviction and sentence of the Plaintiff remains.

Grounds of Appeal

2.4 On 15th June, 2015, grounds of appeal to the conviction of the Plaintiff were delivered which included at grounds 5 and 6 that:-

"*The learned trial judge erred:*

(i) [I]*n admitting into evidence call data records in relation to the mobile phone of the* [Plaintiff] *and other mobile phones attributed to him in circumstances where the statutory regime governing the retention and access to such records was in breach of the appellant's rights pursuant to articles 7 and 8 of the Charter… and equivalent rights*" under the Constitution and the ECHR.

(ii) [I]*n the manner in which he approached the* [decision of the ECJ in *Digital Rights* and] … *in disputing the logic underlying same and substituting his own views in circumstances where he was bound by the decision*."

This appeal awaits to be heard.

Timing of these proceedings

2.5 The Plaintiff was arraigned and pleaded not guilty on 19th January, 2015. On that same day, these proceedings were commenced by the issue of a plenary summons which sought various reliefs as summarised above.

2.6 The facility to challenge legislation while facing a criminal trial poses practical difficulties. The point may not arise because the evidence may not be led by the prosecution or might be excluded by the trial judge in addition to the possibility that the accused may be acquitted. In each of those circumstances, the basis for a challenge as now mounted by the Plaintiff may not present itself.

2.7 Humphreys J. in *North East Pylon Pressure Campaign Ltd v. An Bord Pleanála* [2016] IEHC 300 (Unreported, High Court, 12th May, 2016) summarised as follows:-

"*Thus, a challenge to the constitutionality or ECHR compatibility of legislation does not in general crystallise until the challenger has been subject to the law in question; or in the criminal context until the defendant has actually been convicted and has*

exhausted the criminal process (see my decision in Casey v. D.P.P. *[2015] IEHC 824 (Unreported, High Court, 21st December, 2015)). To* require *a challenge earlier would imperil the right to an effective remedy under Article 40.3 of the Constitution, art. 47 of the EU Charter, art. 13 of the ECHR and art. 2(3)(a) of the ICCPR, which (while not of course part of Irish law) is of persuasive authority in interpreting the foregoing.*" (para. 158).

2.8 In *Kennedy v. DPP* [2007] IEHC 3 (Unreported, High Court, 11th January, 2007) (***"Kennedy"***), MacMenamin J. considered an application for judicial review by a public servant who was alleged to have received a gift from a person with an interest in the discharge of his duties. The applicant sought a declaration that s. 4(1) of the Prevention of Corruption (Amendment) Act 2001 (**"Prevention of Corruption Act"**) which deemed a gift received by the accused in the scenario described "*to have been given and recovered corruptly*…", was unconstitutional and incompatible with the State's obligations under the ECHR as provided for under the European Convention on Human Rights Act 2003 (**"ECHR Act"**) in advance of his trial at the Circuit Criminal Court.

2.9 In *Kennedy*, the accused was actually acquitted and the constitutional challenge was unnecessary. However, the following points extrapolated from *Kennedy* which cited *C.C. v. Ireland* [2006] 4 I.R. 1 extensively, may assist an appreciation of the need for these plenary proceedings:-

(i) It is inappropriate to seek pre-emptively in advance of a trial an interpretation of the law by way of judicial review proceedings;

(ii) The proper forum for the determination of legal matters is at the trial subject to an appeal;

(iii) "*The overwhelming responsibility reposed by the law and the Constitution on the trial judge is to ensure the fairness of the trial. … inherent in that function*

[is] … *the power to judge the validity of legal procedures taken in order to extract, collect or gather evidence*." (para. 29, citing *Blanchfield v. Hartnett* [2002] 3 I.R. at 207 – Fennelly J.)

(iv) Judicial review is not available at all in respect of a trial pending in the Central Criminal Court (the High Court);

(v) Mr. Kennedy, in impugning s. 4(1) of the Prevention of Corruption Act, contended that it was "*a disproportionate statutory means to attain its objective*" which thereby rendered it constitutionally invalid. "… [A]*ny proper consideration of that issue (should it arise)*" required evidence "*concerning the applicability or otherwise of public policy considerations, or other consideration of the common which might constitutionally justify the impugned legislation*". (para. 41).

2.10 Mr. Murray SC for the Attorney General accepted that these proceedings which challenge domestic statutory provisions under the Constitution, EU and ECHR law "*are the necessary and appropriate vehicle for doing that certainly in cases where an assessment of proportionality has to be undertaken with expert evidence…*". As there is a qualified acceptance that this plenary action is appropriate, the battle ultimately pertains to the actual reliefs sought.

2.11 The timing of the Plaintiff's challenge is not an issue for this Court even though the Defendants reserved their position for appeal and other cases. This Court was urged to adjudicate upon all arguments so that clarity can be established as far as possible without having to return to a court of first instance.

2.12 Having said that, this Court respectfully agrees with the reasoning of Costello J. in *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources* [2017] IEHC 307 (Unreported, High Court, 19th July, 2017), where she refused an application

for a preliminary trial following the return of the litigation to the Irish courts after the ECJ delivered its judgment. At para. 26 she confirmed that the challenge could not be tried "*in vacuo*".

2.13 However, the hearing before this Court was neither an application for a trial of a preliminary issue nor was it a preliminary hearing. It was a full plenary trial. Both parties insisted that they do not want to squander the significant resources and time spent on these proceedings. They referred to a desire not to waste the Court's time also when asking for a determination on so many issues.

Issue Estoppel

2.14 Mr. Murray submitted that "…*because of the uncertainty around the status of estoppel in criminal proceedings … it would be wasteful at the end of the day of this Court's time …*" to determine whether Hunt J. had found in the *voir dire* an absence of engagement with the Charter. In other words, there was a consensus that this Court should consider, without reference to the reasons of Hunt J. to admit the evidence from the relevant retained data, the compatibility with EU law of the enactment and operation of s. 3 of the 2011 Act which provided for general retention of telephony data for two years.

Witnesses

2.15 Various facts and documents were agreed prior to the commencement of the hearing in this Court. The Defendants contend that the Plaintiff did not lead any factual evidence about effect or proportionality. Counsel for the Plaintiff relies on the evidence of Mr. Dunphy, solicitor for the Plaintiff, as well as his cross-examination of witnesses called at the request of the Defendants. Counsel contends that this evidence demonstrates that the Irish

regime is in fact general and indiscriminate, allowing certain State authorities to build a profile of a person using his or her movements.

2.16 Undoubtedly the aim of the Defendants in adducing so much evidence was to persuade this Court to undertake its own proportionality assessment of the 2011 Act. The following four witnesses gave evidence as so to fact about retention and access for investigations and particularly relating to the disappearance of the Victim. The other two witnesses, who practise in the UK**,** principally appraised the Court about the utility of retention of and access to mobile telephony data particularly.

Conor O'Callaghan

2.17 Conor O'Callaghan is an electronic engineer who assists and liaises on behalf of service providers with authorities identified in the 2011 Act. Service providers in Ireland adopt a common approach to data retention which is exemplified by a memorandum of understanding dated 4th May, 2011.

2.18 Mr. O'Callaghan explained how service providers typically hold two types of information:-

(i) In the case of bill pay customers, details for invoicing and VAT in addition to verification documentation by personal identification and utility bills;

(ii) Network performance data for engineering, network optimisation and forecasting purposes. The processing of this type of data at a subscriber level is limited by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

2.19 The telephony data which service providers must retain for two years by virtue of s. 3(1) is not necessary for the operations of service providers.

2.20 Further, the Court was told how masts, azimuths, transmissions and calls have a useful but limited way of locating at particular times the position of a phone which sends or receives a call or text. Users of apps on the internet (such as web mapping services) in comparison, readily identify and use location data. In those circumstances the user expressly consents to tracking or locating details on a particular device or app which uses the internet. On the other hand, those who make or receive calls or texts generate the telephony data that is retained for two years solely as a result of the 2011 Act. Other tracking type data may be stored on a device or elsewhere according to the agreement between the subscriber and the service provider.

Sarah Skedd

2.21 Senior crime and policing analyst, Sarah Skedd whose methodical and wide-ranging analysis of the mobile phones relevant to the investigation of the Victim's disappearance demonstrated the benefit and necessity of her expertise and work.

DCS Peter Kirwan

2.22 Retired DCS Peter Kirwan explained the factual position which pertained before and during the investigation leading to the conviction of the Plaintiff. The later chronology in this judgment shows how he was aware of telephony data requests for a number of phones which fed into his assessments for the requests which centred on the 407 phone. The painstaking investigation while adhering to the principles of fairness and having regard to privacy rights as then understood was impressive. The overview of the system for access as given by DCS Kirwan appears at para. 3.88 of this judgment.

DCS Anthony Howard

2.23 DCS Anthony Howard, who has had extensive operational experience investigating serious organised crime, satisfied this Court that retained data has been critical in many investigations of serious crimes. He emphasised internal Garda procedures which address the proportionality and necessity of measures taken before accessing retained data.

David Anderson QC

2.24 David Andersen QC, who with his breath-taking experience reviewed "*the operation and regulation of investigatory powers*", before producing a report for the Prime Minister of the UK entitled "A Question of Trust" in his capacity as Independent Reviewer of Terrorism Legislation pursuant to s. 7 of the Data Retention and Investigatory Powers Act 2014 (**"DRIPA"**). He gave evidence to this Court about the utility of retained data and the absence of effective alternatives to a general data retention regime in the fight against serious crime. Mr. Anderson identified:

(i) the option of data preservation orders (so called "*quick freeze*") which has little benefit for investigations that do not have an immediate suspect; and

(ii) the diminishing advantage for investigations as time elapses from generation of data less than three months old (72% benefit) to data older than twelve months (3% benefit).

Professor Michael Clarke

2.25 Michael Clarke, Professor of Defence Studies and a specialist adviser to the House of Commons Defence Committee since 1997, chairman of an independent surveillance review for the Royal United Service Institute and an expert witness in a number of terrorism related trials in the UK among many other remarkable contributions, distinguished mass surveillance

of the entire population with the retention of data used in the Plaintiff's criminal trial. Professor Clarke pointed to the "*inert*" nature of the retained data. Surveillance, he explained, only occurs when some part of retained data is examined. He outlined how discriminate targeting as opposed to indiscriminate surveillance is achieved by the layers and steps involved in retention by a mobile telephone provider with accountable internal precautions, the inability to match data to subscriber data without other safeguards and a much restricted and regulated access to such data. Professor Clarke demonstrated his independence when he opined that the data regime in the UK was "*general and indiscriminate*". On cross-examination in this Court, he conveyed his understanding that the Irish retention provisions are as broad as those in the UK in answer to the question about whether the Irish regime is "*general and indiscriminate*".

Court's observations

2.26 Mr. O'Callaghan and other witnesses assisted the Court which now allows it to make the following observations that inform its deliberation:-

(i) Section 4 provides for security of the telephony data within the control of service providers. The Plaintiff does not complain in these proceedings that a service provider breached s. 4. However, submissions were made on his behalf about the lack of clarity relating to the monitoring and sanctioning of breaches of the 2011 Act.

(ii) The immediate privacy of mobile phone users is not compromised by the actual retention of data by the service providers pursuant to their obligations under the 2011 Act. The intrusion can occur after the extraction of the data is interpreted with the help of separate details available to service providers. The mobile telephony data unprocessed without cell site coordinates available to

service providers reveals nothing other than that an event such as a call, text or data session occurred. A binary task is required to obtain any meaning from the telephony data. Linking the details is done manually by an engineer such as Mr. O'Callaghan. A radio planning tool can be applied which has a 3D view of the country with all the contours showing hills and mountains. Mr. O'Callaghan confirmed that he in that role does not know the name of the individual being tracked.

(iii) Connecting the number with the details for the acquisition of that number is a separate process. Bill pay customers create easily accessible subscriber information and pay as you go phones generate details about when, where and how phones and credit are procured by the user. The term "*dirty phone*" applies to phones used in criminal activity which are generally pay as you go phones.

(iv) Service providers have different sections which segregate and secure access to the data that may be requested under the 2011 Act. In brief, there are statutory requirements to be fulfilled and operational arrangements to be undertaken which safeguard the identity of mobile users until after the binary task is completed. Furthermore, the disclosure of subscriber details is a separate process. More particularly the binary task requires manual input by an experienced and trained individual such as Mr. O'Callaghan.

(v) Algorithms and other technical means can sift through masses of data to a point where specific inferences can be drawn, according to Professor Clarke and commented upon by Mr. Anderson. The ever-increasing capacity and speed to process this type of data enhances investigatory powers greatly. In

other words manual input can precede, be used in and follow upon the application of algorithms and other scientific or mathematical formulae.

(vi) The 2011 Act does not facilitate a retrospective following of a mobile device user. If there are different calls, texts or data sessions between masts it may be possible to pinpoint use but it will not follow a user. This is in contrast to the ability of a service provider in a hostage situation, for example, to "*ping*" a device for its latest point of connection with or without a call.

(vii) Mr. O'Callaghan believes that breaches by service providers of their obligations under the 2011 Act are treated very seriously and that there is a role for the DPC in that context.

(viii) In answer to a question from the Court, Mr. O'Callaghan cautiously accepted that there are now alternatives to locating the whereabouts of an individual who uses a device at a particular time. He acknowledged that text messaging is "*vastly*" decreasing. Other witnesses also mentioned that those aged under 35 particularly engage more with the internet for communicating. Therefore, the relevance and necessity of telephony data for the investigation of crime may be dissipating due to the exponential decrease in the numbers using voice calls and texts only. In that context, it is this Court's view that the specific facts giving rise to the claim of the Plaintiff in these proceedings involving the 407 phone may not be replicated as often as before. There was little debate about the retention and access to internet data defined in Schedule 2, Part 2 of the 2011 Act which is retained for one year.

Chronology

2.27 The Court has prepared the following chronological outline of relevant legislation and cases together with details of the investigation and the prosecution of the Plaintiff because it formed the background for the submissions made and in preparing this judgment. It is set out for ease of understanding by those with particular interest in one or other of the facets identified in submissions and given the quick-moving sequence of relevant judgments and reviews up to the date of delivery of this judgment. This chronology also contains facts emphasised by one or other of the parties which are not necessarily relevant to understanding the ultimate conclusions of this Court. The facts are chosen to assist in portraying an overall view of the criminal trial and outstanding appeal in the background of this litigation. Terms and words are highlighted in this judgment for ease of reference:-

24.10.98 The deadline for Member States to transpose the 1995 Directive. At the risk of over simplification, personal data could only be kept according to this Directive where it was necessary for customers or suppliers. Recital 2 of the 1995 Directive read:-

> "*… data-processing systems are designed to serve man … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;*"

25.5.2018 was the deadline for implementation of the General Data Protection Regulation (**"GDPR"**) which replaces the 1995 Directive and enhances the protection of data privacy. The GDPR postdates all events relevant to this case.

31.10.03	The deadline for Member States to transpose the 2002 Directive. The 2002 Directive did not address lawful interceptions but sought to harmonise the rules for the processing of personal data while allowing for an exception to retain data, including telephony data, in certain enumerated circumstances.
31.12.03	Commencement of the ECHR Act in Ireland.
15.09.07	The deadline for the transposition of the **2006 Directive** which altered the harmonising rules for retained data and introduced obligatory measures for accessing the retained data.
13.12.07	Treaty of Lisbon signed by Member States.
2008 –2009	Records for this period kept by the Plaintiff's then employer showed 847 text messages from the 407 phone to the iPhone of the Victim; these messages do not fall within the challenged retained data.
09.02.09	The ECJ in *Ireland v. Parliament* dismissed the challenge by Ireland to the legal basis for adopting the 2006 Directive.
26.11.09	The ECJ in *Commission v. Ireland (Case C-202/09)* [2009] E.C.R. I-203 (***"Commission v. Ireland"***) held that by failing to adopt the provisions necessary to comply with the 2006 Directive, Ireland had failed to fulfil its obligations under that Directive.

01.12.09 Treaty of Lisbon entered into force.

05.05.10 McKechnie J. granted Digital Rights Ireland Limited "*locus standi to bring actio popularis*", [2010] 3 I.R. 251. He decided to make a reference to the ECJ under Article 267 of the TFEU which resulted in the judgment in *Digital Rights* on 08.04.14 declaring the 2006 Directive to be invalid.

26.01.11 The 2011 Act was enacted and commenced.

04.05.11 A Memorandum of Understanding between the communications industry and An Garda Síochána and other authorities was finalised for co-operation in handling retained data and other data under the 2011 Act (**"MoU"**).

22.08.12 The Victim went missing, according to the evidence adduced at the criminal trial of the Plaintiff.

26.08.12 A request was emailed to Detective Chief Superintendent Peter Kirwan, in charge of security and intelligence section at Garda Headquarters in the Phoenix Park, (**"DCS"**). The email set out suspicious circumstances in relation to the Victim's sudden disappearance and requested retained data for the period from 5pm on 22.08.12 to 3pm on 23.08.12 in respect of the Victim's iPhone. A

mobile number (**"474 mobile"**) had sent lurid texts to the Victim's iPhone up to 12.07.12.

27.08.12 The DCS requested "*all data*" in accordance with s. 6 of the 2011 Act for the Victim's iPhone from five mobile phone operators.

08.10.12 The DCS requested "*all data*" for the 474 mobile for the period 00:00 on 22.08.12 to 24:00 on 04.10.12 following a similar request which had been changed after the Telecoms Liaison Unit (**"TLU"**) advised that further details were required.

25.02.13 Directives issued by the Assistant Commissioner of An Garda Síochána set out the procedures for making requests to the TLU and the DCS under the 2011 Act and otherwise (**"2013 Garda HQ Directives"**) which repealed directives (issued in 2008 prior to the 2011 Act) concerning necessity, proportionality and appropriateness considerations for telecommunication data requests.

13.09.13 Remains of the Victim were found in the Dublin Mountains according to the evidence adduced at the criminal trial.

16.09.13 Keys belonging to the Victim were found at Vartry Reservoir after an angler had brought items to a Garda Station. A garda went to the scene of the discovery and found two Nokia phones described at the criminal trial as the "**master**" and "**slave**" phones in the reservoir and these

were attributed (without acceptance by the Plaintiff) by investigators to the Plaintiff and the Victim respectively. A printout of text messages between these two phones was exhibit 318 at the criminal trial. A supermarket loyalty card traced to the Victim was also found at the reservoir.

02.10.13 An investigating garda in Blackrock, Co. Dublin, set out in writing the background and reasons for making the requests for the retained data for the 474 phone pursuant to the 2011 Act to the DCS.

03.10.13 The DCS received one of the applications with the grounds and reasons for the retained telephony data in respect of the 407 number from 23.08.12 – 30.11.12 pursuant to s. 3 of the 2011 Act.

04.10.13 The DCS reviewed two further similar applications in respect of the retained telephony data for the 407 number for three periods: 07.10.11 – 31.12.11, 01.01.12 – 31.03.12, and 01.04.12 – 31.05.12. DCS Kirwan testified at the criminal trial and before this Court that he was satisfied about the necessity and appropriateness of the records for the investigation of serious criminal activity and that they accorded with s. 6(1) of the 2011 Act.

15.10.13 The senior crime and policing analyst, Ms. Skedd, having analysed the retained data which had been procured, handed documents to the Detective Garda who later interviewed the Plaintiff. These included a

map and other details showing cell usage for the 407 number which supported, *inter alia*, the increasing attribution by the investigators for the use by the Plaintiff and the Victim of the master and slave phones.

17.10.13 The Plaintiff was arrested and, following caution, answered questions including that he used the GPS on the 407 phone. Following an extension of the detention period and in further questioning, the Plaintiff was told of the use by the investigating gardaí of retained telephony data for the 407 phone and CCTV footage. In one reply, the Plaintiff stated:

> '*… you're making huge assumptions. I'd like you to use that phone technology to see where my phone was wherever you think is significant*.'

A third interview of the Plaintiff dealt more extensively with the retained data for the purpose of obtaining the Plaintiff's response to the investigators' attribution of the master phone.

18.10.13 The Plaintiff was charged with the murder of the Victim.

12.12.13 Advocate General Cruz Villalón delivered his Opinion in *Digital Rights* in which he suggested the suspension of "*the effects of the finding that Directive 2006/24 is invalid pending adoption by the European Union legislature of the measures necessary to remedy the invalidity found to exist…*" (para. 158). The EU legislature has not adopted any such legislation since 2014 (ECLI:EU:C:2013:845).

29.01.14 The book of evidence was served on the Plaintiff.

08.04.14 The ECJ delivered judgment in *Digital Rights* declaring the 2006 Directive invalid and it did not address the suspension proposal of Advocate General Cruz Villalón.

26.08.14 The Plaintiff's solicitor wrote to the prosecution solicitor repeating a request for "*details of relevant cell sites*", noting that a recent ECJ judgment cast doubt over the use of retained data in criminal trials, before asking whether evidence of cell site analysis will be adduced at trial because it was included in the Book of Evidence. The prosecution's solicitor clarified that it was always open for the prosecution to clarify that it would not lead that evidence and that the Plaintiff's legal advisers should have the opportunity in advance of the trial to make a submission about the inadmissibility of the retained data.

05.12.14 The Plaintiff's solicitor noted in a letter to the prosecution's solicitor that the Director of Public Prosecutions (**"DPP"**) had in a recent murder case decided not to rely on retained data.

12.12.14 The prosecution solicitor replied with confirmation that as of that "*juncture*" the retained telephony data would be relied upon.

19.01.15 The plenary summons for these proceedings was issued and the Plaintiff pleaded 'not guilty' at his arraignment.

20.01.15 The criminal trial of the Plaintiff commenced.

Feb 15 Evidence and submissions were led in the *voir dire* before Hunt J. on days 24 and 25 of the criminal trial.

25.02.15 Hunt J. ruled that the retained data was admissible.

27.03.15 The Plaintiff was convicted by the jury for murder.

15.04.15 The Supreme Court delivered judgment in *J.C.*.

29.04.15 The Administrative Court of Appeal in Stockholm made a reference under Article 267 TFEU concerning the compatibility of 2012 Swedish legislation, which sought to transpose the 2006 Directive, having regard to Articles 7, 8 and 52(1) of the Charter. This arose after Tele2 Sverige AB on 09.04.14 informed the Swedish Post and Telecom authority that it would no longer **retain** data due to the effect of *Digital Rights*.

20.11.15 The Court of Appeal of England and Wales in *Secretary of State for the Home Department v. Watson & others* [2018] Q.B. 912; [2018] EWCA Civ 70 (**"2018 Watson judgment"**) made a reference to the

ECJ seeking clarification on whether *Digital Rights* laid down mandatory requirements of EU law applicable to the domestic regime of a Member State governing access to retained data in order to comply with Articles 7 and 8 of the Charter.

22.12.15 The statement of claim was delivered in these proceedings.

Jan 2016 Following media reports about access to telephone records of journalists, the Government engaged former Chief Justice Murray to review the law on the retention and access to communications data (**"Murray Review"**).

19.07.16 Advocate General Saugmandsgaard Øe delivered his Opinion in the joined cases of *Tele2* and *Watson*. At para. 7 he said:-

> "*I have the feeling that a general data retention obligation imposed by a Member State may be compatible with the fundamental rights enshrined in EU law provided that it is strictly circumscribed by a series of safeguards…*".

(ECLI:EU:C:2016:572).

05.10.16 The defence in these proceedings was delivered.

21.12.16 The ECJ delivered judgment in *Tele2* and did not place any temporal limitations on its decision.

16.05.17 Notice of trial was served in these proceedings.

26.09.17 The Investigatory Powers Tribunal (**"IPT"**) in the UK made a determination in *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and others* [UK IP Trib IPT_15_110_CH] (**"2017 IPT judgment"**) on the effect of *Tele2* on acquiring Bulk Communications Data (**"BCD"**) pursuant to the Telecommunications Act 1984 followed by an order for a preliminary reference to the ECJ about whether BCD for the national security of the UK falls within the remit of EU law.

03.10.17 The Minister for Justice and Equality published the Murray Review with a link to the General Scheme of the Communications (Retention of Data) Bill 2017 which came before the Oireachtas Joint Committee on Justice and Equality on 08.11.17 and 15.11.17.

15.11.17 According to a transcript produced to this Court of a hearing in *DPP v. O'Driscoll*, McCarthy J. in the Central Criminal Court (**"McCarthy ruling"**) ruled in favour of the admissibility of telephony data despite his view that there was a breach of "*the rights of the accused in community law*". McCarthy J. explained that the DCS "*acting with upmost good faith*" had also "*acted on the basis of the law of the land as it then stood … and that this is a case where I should receive this evidence by virtue of the discretion extended by*" *J.C.*.

12.12.17 Within the European Agenda on Security, the European Commission's 'Twelfth progress report towards an effective and genuine Security Union' [COM (2017) 779 final] mentioned, on p. 11, that the recent Joint Home Affairs Council meeting had "*decided to continue discussions at expert level with a view to finding a common understanding of possible solutions on data retention in line with the Tele2 ruling…*". The thirteenth (21.01.2018), fourteenth (17.04.2018) and fifteenth (13.06.2018) progress reports have not provided updates in relation to these discussions.

30.01.18 The Court of Appeal of England and Wales in the 2018 Watson judgment declared that s. 1 DRIPA "*was inconsistent with EU law to the extent that, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, it permitted access to retained data:-*

> *(a) where the object pursued by that* ***access*** *was not restricted solely to fighting* ***serious crime****; or*
>
> *(b) where* ***access*** *was not subject to* ***prior review by a court or an independent administrative authority***." (para. 27, emphasis added by this Court).

01.02.18 The Joint Committee on Justice and Equality delivered its 'Report on Pre-Legislative Scrutiny of the Communications (Retention of Data) Bill 2017' and the legislation was scheduled in the priority list for enactment in 2018.

20.02.18 The Court of Appeal delivered judgment in *DPP v. Gary Flynn* [2018] IECA 39 (Unreported, Court of Appeal, 29th February, 2018) which dismissed the defendant's appeal from his conviction for murder on the grounds, *inter alia*, that investigating Gardaí wrongly accessed location data of mobile phones during their investigations:-

> "*The Court regard*[ed] *as risible the suggestion that evidence accumulated during an investigation into an offence as serious as murder with a firearm should in circumstances of this case be excluded to discourage Garda misconduct. In any event there was no Garda misconduct here*."

24.04.18 The European Court of Human Rights (**"ECtHR"**) delivered judgment in *Benedik v. Slovenia* (App. No. 62357/14, ECtHR, 24th April, 2018) (***"Benedik"***). This discussed the interference with the right to privacy "*in accordance with law*" that may be pursued as "*necessary in a democratic society*" of a participant charged with involvement in a network providing child pornography.

27.04.18 The High Court of England and Wales delivered judgment in *R (on the application of National Council for Civil Liberties (Liberty)) v. Secretary of State for the Home Department* [2018] EWHC 975 (Admin); [2018] 3 W.L.R. 1435, on Liberty's challenge to Part 4 of the Investigatory Powers Act 2016 (**"IPA 2016"**), (***"Liberty"***). That Court declared two provisions to be incompatible with EU law and that those

incompatibilities should be remedied by 01.11.18. The Court refused Liberty's application for a reference about whether retaining communications is a "*general and indiscriminate privacy violation*" to the ECJ but stayed that part of its claim pending the decision of the ECJ in the reference by the IPT of 08.09.17 concerning "*national security*".

03.05.18 Advocate General Saugmandsgaard Øe delivered his Opinion in *Ministerio Fiscal (Case C-207/16)* ECLI:EU:C:2018:300 (***"Ministerio Fiscal"***), a preliminary reference from the Spanish courts seeking clarification on the interpretation of 'serious crime' in *Tele2*. The Defendants rely on this Opinion when contending for a narrow interpretation of *Tele2*.

19.06.18 The ECtHR in *Centrum för Rättvisa v. Sweden* (App. No. 35252/08, ECtHR, 19th June, 2018) found that, despite deficiencies in notifying individuals of surveillance, the Swedish law met the high protecting threshold for bulk interception of communications.

22.06.18 The United States Supreme Court did not address the legality of retention when delivering a 5-4 judgment in *Carpenter v. United States* 585 U.S. ___ (2018) (***"Carpenter"***) which emphasised constitutionally compliant access protocols for data retained.

05.07.18 Counsel for the parties made final oral submissions following this Court's request on 20.04.18, about prospective and retrospective effects in view of the emerging law internationally.

16.07.18 The transcript of a ruling in *DPP v. Jason O'Driscoll* by White J. in the Central Criminal Court (**"White ruling"**) which led to murder convictions mentioned:-

a) there was a presumption of constitutionality attaching to the 2011 Act and

b) at the time the relevant data was retained in 2012 the 2006 Directive had not yet been declared invalid by the ECJ.

White J. stressed that it should not be taken "*that evidence obtained in circumstances of illegality should readily be admitted*".

13.09.18 The ECtHR in *Big Brother Watch and others v. the UK* (App. Nos. 58170/13, 62322/14 & 24960/15, ECtHR 13th September, 2018) (***"Big Brother Watch"***) found a violation of Article 8 of the ECHR because, among other considerations, the impugned legislation had been acknowledged by the UK as violating fundamental rights in EU law. Briefly, the UK concession that the legislation was not limited to "*serious crime*" and that access to retained data did not have to undergo "*a prior review by a Court or an administrative body*" meant that the legislation was not in accordance with EU law and ultimately UK law.

25.09.2018 The ECJ accepted a reference made under Article 267 TFEU from the Cour constitutionelle (Belgium) (*Ordre des barreaux francophones et germanophone & Others (Case C-520/18)*) which arises from an action to annul a 2016 law repealing 2013 laws that transposed the invalid 2006 Directive. The Defendants in their cover note lodged with this Court on 12.10.2018 highlighted that the Belgian Court asked whether legislation is precluded where the object is to comply with the positive obligations under Articles 4 and 8 of the Charter which require effective investigation and punishment of child sex offences. The summary of the ECJ's acceptance at para. 118 refers to material available to the referring court which makes it apparent that most Member States have had great difficulty with ensuring that their data retention laws are compatible with the case-law of the ECJ. The Cour constitutionelle also asks whether, if the legislation is declared invalid, it might retain the effects of the law on a temporary basis in order to avoid legal uncertainty and to enable the data previously collected and retained to continue to be used for the objectives pursued by the law.

02.10.2018 The ECJ delivered judgment in *Ministerio Fiscal*. This case involved access to retained data to identify the owners of SIM cards activated with stolen mobile telephones. The ECJ found that national legislation did not require that access be limited to the objective of fighting "*serious crime*" where the interference itself is not serious. This followed the Advocate General's Opinion given on 03.05.18 (ECLI:EU:C:2018:788).

02.10.2018 The ECJ accepted a reference from the Conseil d'État (France) (*Quadrature du Net & Others (Joined Cases C-511/18 and C-512/18)*) which included of particular relevance, according to the Defendants' note lodged with this Court on 12.10.2018, the question whether a "*general and indiscriminate obligation*" may be justified by reference to the right to security guaranteed in Article 6 of the Charter and the requirements of national security which is the sole responsibility of the State under Article 4 TFEU.

08.11.2018 The transcript of the ruling by White J. in the murder prosecution, *DPP v. Tynan and Fitzgerald* (Bill No: CCDP 14/2017) at the Central Criminal Court reveals how mobile phone call data, location and activation data of pre-paid mobile phones which had been sought in an investigation after the delivery of *Digital Rights* in April 2014 and before the judgment in *Tele2* in December 2016 was deemed admissible as evidence (**"second White ruling"**). White J. examined "*the facts surrounding the evidence sought to be excluded to assist…*" the application of the *J.C.* test.

Order of Discussion

2.28 In *Carmody v. Minister for Justice* [2010] 1 I.R. 635 (**"*Carmody*")** the Supreme Court held that the inability of a declaration of incompatibility with the ECHR to resolve the issues between the parties meant that the constitutional point raised ought to have been decided first. However, the Supreme Court clarified, at para. 43, that the order for determination of issues

was ultimately a matter for the trial Court. Mr. Farrell SC for the Plaintiff, in reply to this Court's question, expressed reluctance to have this Court embark on a "*constitutional analysis*" if an effective declaratory remedy without a temporal restriction is made.

2.29 I conclude that it is preferable to address EU law first followed by and combined with the ECHR law about access to "*retained data*". Any constitutional question which remains can then be decided having had the benefit of a discussion about prospective, retrospective and suspensory effects of the remedies sought in these proceedings.

2.30 The reason for selecting ECHR law in that order is that the ECHR law enhances the embryonic-like status of EU law for access to data. The Court notes in this regard Article 52(3) of the Charter:-

> "*In so far as this Charter contains rights which correspond to rights guaranteed by the* [ECHR], *the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*"

2.31 The necessity for consistency between the interpretation of the Charter and the ECHR is noted at p. 33 of the Explanations for the Charter. A practical application of this principle is found in the recent case concerning the derived rights of same sex spouses involving citizens of the European Union: *Relu Adrian Coman and Others v. Inspectoratul General pentru Imigări and Ministerul Afacerilor Interne (Case C-673/16)* (ECLI:EU:C:2018:385). The ECJ in considering the definition of "private life" in Article 7 of the Charter noted that it was apparent from the explanations to the Charter that:-

> "*… in accordance with Article 52(3) of the Charter, the rights guaranteed by Article 7 thereof have the same meaning and the same scope as those guaranteed by Article 8 of the* [ECHR]." (para. 49).

3. EU LAW

Primacy of EU Law

3.1 The primacy of EU law has long been a cornerstone principle of case law as a result of the 3rd and 29th amendments of the Constitution in 1972 and 2009 respectively, when Ireland became part of the European Economic Community and then the European Union.

3.2 It is well-established that EU law has primacy over national laws, including national constitutional principles (*Flaminio Costa v. E.N.E.L. (Case 6/64)* [1964] ECR 585; *Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel (Case 11/70)* [1970] ECR 1125). Thus, a national law which is found to be inconsistent with EU law must be disapplied by the national court (*Amministrazione delle finanze dello Stato v. Simmenthal (Case 106/77)* [1978] ECR 629 (***"Simmenthal"***)) and a national constitutional law cannot be invoked to challenge an EU law. However, the ECJ has recognised that "*respect for fundamental rights forms an integral part of the general principles of community law protected by the Court of Justice*" (*Internationale Handelsgesellschaft*) and that the application of EU law in Member States can be scrutinised by reference to the fundamental rights recognised at an EU level (*Rutili v. Minister for the Interior (Case 36/75)* [1975] ECR 1219).

3.3 In *Wachauf v. Germany (Case 5/88)* [1989] ECR 2609, the ECJ held that Member States must ensure the protection of fundamental rights whenever the Member State implements an EU measure. In this way, the Member States are "*agents*" of the EU when implementing EU law. The ECJ has defined 'implementing EU law' quite broadly to also include measures derogating from EU law (*ERT v. DEP (Case C-260/89)* [1991] ECR I-2925).

3.4 The fundamental rights recognised at the EU level were codified in the Charter of Fundamental Rights, which was approved by Member States in December 2000. The legal

status of the Charter was left vague in anticipation of the constitutional processes that were commenced at that time but eventually the Charter was incorporated into the Lisbon Treaty with Article 6(1) TEU providing:-

> "*The Union recognises the rights, freedoms and principles set out in the* [Charter] *which will have the same legal value as the Treaties*."

3.5 Article 51(1) of the Charter applies the Charter to Member States "*when they are implementing Union law*." The ECJ in *Åklagaren v. Åkerberg Fransson (Case C-617/10)* (ECLI:EU:C:2013:105) interpreted 'implementing' and confirmed its earlier approach of an expanded scope of application of the Charter. Thus, national laws which fall within the scope of EU law must comply with the rights provided by the Charter.

The Key Cases

3.6 Following is an introduction and then summaries of the key ECJ judgments most relevant to the Plaintiff's claims in these proceedings.

The Dispute at EU Level

3.7 Article 1(3) of the 2002 Directive (enacted before the introduction of shared competencies including those in the areas of security and criminal law by the Lisbon Treaty) provides that:-

> "*This Directive shall not apply to activities which fall outside the scope of the Treaty … and in any case to activities concerning public security, defence, State security … and the activities of the State in areas of criminal law*."

3.8 On the other hand, Article 15(1) enabled Member States to adopt legislative measures to restrict the rights and obligations provided for in the 2002 Directive:-

> "*… when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may,* inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the* [TEU]."

By way of summary there was a perceived conflict between Article 1(3) and Article 15(1) of the 2002 Directive until *Digital Rights* and *Tele2*.

Digital Rights

3.9 The 2006 Directive had been adopted within the space for Member State action envisaged by Article 15(1) of the 2002 Directive, as a result of the varying approaches to this Article by Member States. The 2006 Directive followed upon a growing realisation that internet and telephony data were valuable in preventing, defeating and prosecuting terrorist and criminal offences (Recital 7). The period of retention of such data should not exceed two years with corresponding safeguards for access. It specifically disapplied Article 15 of the 2002 Directive (Article 11 of the 2006 Directive) concerning the necessary, appropriate and proportionate test for measures.

3.10 The 2006 Directive laid down the obligations on service providers to retain certain data which was generated or processed by them and to ensure that that data was available for

the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in national law.

3.11 This case arose from references by the Irish High Court in *Digital Rights Ireland Ltd. v. Minister for Communications* and the Verfassungsgerichtshof (Austrian Constitutional Court) in *Seitlinger and Others*. In essence, the referring courts asked the ECJ to examine the validity of the 2006 Directive in light of Articles 7, 8 and 11 of the Charter.

3.12 In doing this the ECJ considered whether the Directive raised questions under the Charter; whether there was an interference with the rights under Article 7 and 8, and whether that interference was justified having regard to the principle of proportionality as articulated in Article 52(1) of the Charter.

Application of the Charter

3.13 The ECJ considered that the obligation on service providers to retain data for the purpose of making it accessible to the competent national authorities did raise questions under Articles 7 and 8. In that respect, the ECJ noted that the data to be retained:-

> "*make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.*
>
> *Those data, taken as a whole, may 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.*" (paras. 26-27).

Was there an interference?

3.14 The ECJ continued that the 2006 Directive derogated from the system of protection of the right to privacy and confidentiality of communications established by the 1995 and 2002 Directives in the context of the processing of personal data in the electronic communications sector. Therefore, the obligation on service providers to retain and process data relating to a person's private life and to his/her communications constituted in itself an interference with Articles 7 and 8. The access of the competent national authorities to such data constituted a further interference. The ECJ commented that the interference caused by the Directive was wide-ranging and particularly serious and that "*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*." (para. 37).

Was the interference justified?

3.15 Referring to Article 52(1) of the Charter, the ECJ explained that any limitation on rights had to be provided for by law and respect the essence of those rights. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or meet the need to protect the rights and freedoms of others. The ECJ held that the interference did satisfy an objective of general interest: the material objective of the Directive was to contribute to the fight against serious crime and ultimately to public security.

3.16 The ECJ next considered the proportionality of the interference. The principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives. The ECJ held that in this case, in view of the

important role played by the protection of personal data in light of the right to respect for private life and the extent and seriousness of the interference with that right, the EU legislature's discretion was reduced. Thus the ECJ had to conduct a strict review of that discretion.

3.17 Having regard to the question of appropriateness, the ECJ acknowledged that the retention of data is a valuable tool in criminal investigations and must be considered appropriate for attaining the objective of the Directive.

3.18 Under the necessity criterion, the ECJ held that the fight against serious crime is of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, the ECJ found that even this fundamental objective of general interest could not justify the retention measure established by the 2006 Directive.

3.19 The ECJ held that the protection of fundamental rights requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. As such, the EU legislature must "*lay down 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 risk of abuse and against any unlawful access and use of that data*" (para. 54). The ECJ added that the need for such safeguards is all the greater where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data, as in the 2006 Directive.

3.20 In considering whether the interference was limited to what was strictly necessary, the ECJ mentioned that the obligation to retain applied to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. The 2006 Directive covered all subscribers and registered users and thus entailed an

interference with the fundamental rights of "*practically the entire European population*." (para. 56). In this regard, the ECJ said that no distinction was made for persons for whom there is no evidence capable of suggesting even a remote or indirect link with serious crime. Thus, no relationship was required between the data whose retention was provided for and a threat to public security.

3.21 The ECJ observed that the 2006 Directive:-

(i) failed to lay down any objective criterion by which to determine the limits to be placed on the access and subsequent use of the data in order to justify the serious interference with fundamental rights;

(ii) did not contain substantive and procedural conditions relating to the access and subsequent use of the data. The purpose was not strictly restricted to preventing and detecting precisely defined serious offences;

(iii) did not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained was limited to what was strictly necessary in light of the objective pursued;

(iv) did not make access by the competent national authorities dependant on a prior review carried out by a court or by an independent administrative body;

(v) required the data to be retained for a period of at least six months without any distinction between the different categories of data on the basis of their possible usefulness. There was also no obligation that the determination of the period of retention ought to be based on objective criteria in order to ensure that it was limited to what was strictly necessary.

Conclusion of the ECJ

3.22 For these reasons, the ECJ concluded that the 2006 Directive did not lay down clear and precise rules governing the extent of the interference with the fundamental rights provided in Articles 7 and 8 of the Charter. Thus, the interference was not circumscribed by provisions to ensure that it was limited to what was strictly necessary. The ECJ also found that the 2006 Directive did not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. The lack of a requirement that the data must be retained within the EU was also critical.

3.23 In those circumstances, the ECJ found that the EU exceeded the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter by adopting the 2006 Directive and the Directive was declared invalid.

Complication of Invalid 2006 Directive

3.24 This declaration of invalidity of the 2006 Directive in *Digital Rights* reinstated Article 15 of the 2002 Directive and the perceived conflict re-emerged.

Tele2

3.25 Requests were made for preliminary rulings by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm) in the case of *Tele2 Sverige AB v. Post- och telestyrelsen* and the Court of Appeal of England and Wales in the case of *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*.

3.26 The case in *Tele2* arose in 2014 when, following *Digital Rights,* Tele2 Sverige, a Swedish provider of electronic communications, informed the Swedish Post and Telecom Authority that as the 2006 Directive was invalid it would cease to retain electronic

communications data covered by the Swedish legislation. This legislation imposed an obligation on providers of electronic communications services to retain the metadata of all telephony services and internet access services for a period of six months. The providers of these services had to disclose data at the request of relevant national authorities if that data was connected with a "*presumed criminal offence*". It was not necessary that this offence be a serious crime.

3.27 When the Authority held that Tele2 Sverige was in breach of its obligations, the latter brought a case before the Swedish Courts. On appeal, the Administrative Court of Appeal, Stockholm, referred two questions to the ECJ:-

(i) Is a general obligation to **retain** traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of the 2002 Directive, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

(ii) Does Article 15(1) of the 2002 Directive, read in light of Articles 7, 8 and Article 52(1) of the Charter, preclude national legislation governing **access** of the competent national authorities to retained data, where:

a. The legislation does not restrict access solely to the objective of fighting serious crime;

b. Access is not subject to prior review by a court or an independent administrative authority; and

c. There is no requirement that the data concerned should be retained within the EU.

3.28 At the relevant time, the provisions for retention and access to data in the UK were to be found under DRIPA and Regulation of Investigatory Powers Act 2000 (**"RIPA"**). Section

1 of DRIPA allowed the Secretary of State to send notices to public telecommunications operators requiring them to retain relevant communications data, without prior authorisation from a court or an independent administrative body. The respondents in *Watson* lodged applications for judicial review of the legality of s. 1 of DRIPA, claiming, *inter alia*, that it was incompatible with Article 7 and 8 of the Charter. The Court of Appeal asked whether *Digital Rights* laid down mandatory requirements of EU law applicable to a Member State's domestic regime governing **access** to data, a question that was addressed along with the second question from the Swedish Court.

The scope of the 2002 Directive

3.29 As mentioned, Article 15(1) of the 2002 Directive remained the governing provision for exceptions to the rule of confidentiality of electronic communications following *Digital Rights*. In determining the scope of the 2002 Directive, the ECJ considered its general structure. Notwithstanding that the legislative measures referred to in Article 15(1) concern activities characteristic of the State or State authorities and pursue public interest objectives overlapping substantially with Article 1(3) of the 2002 Directive (which excludes from the scope of the Directive activities of the State in the areas of, *inter alia*, criminal law and State security), such measures fall within the scope of the Directive, according to the ECJ. Article 15(1) presupposes this since it expressly authorises the Member States to adopt such measures only if the conditions laid down in the Directive are satisfied. Excluding such measures from the scope of the Directive would deprive Article 15(1) of any purpose.

3.30 The ECJ confirmed that legislation concerning retention of data by service providers and legislation providing for access to the data by State authorities both fall within the scope of the 2002 Directive. The protection of the confidentiality of communications and related data guaranteed by the 2002 Directive applies to measures taken by all third parties, whether

private actors or public authorities. Moreover, legislation requiring service providers to grant national authorities access to the retained data involves the processing of personal data by those providers which falls within the scope of the Directive. Since data is retained only for the purpose of making that data available to the competent national authorities, national legislation requiring retention of data necessarily entails the existence of provisions relating to access by the authorities to that data.

3.31 The Court reiterated these conclusions in its recent judgment of *Ministerio Fiscal*. The Court added, in that case, that such measures requiring service providers to grant access, to the extent that they regulate the activities of such providers, cannot be regarded as activities characteristic of States (para. 37).

General findings

3.32 The ECJ interpreted Article 15(1) in the context of the 2002 Directive and the Charter when coming to the following general conclusions:-

(i) The primary function of the 2002 Directive is to ensure a high level of protection of personal data and privacy for users of all electronic communications services. In so far as Article 15(1) enables Member States to restrict the scope of the obligation to ensure the confidentiality of communications and related data, that provision must be interpreted strictly so that the exceptions to the obligation cannot become the rule and render the latter largely meaningless.

(ii) In providing the only exceptions, the list of objectives in Article 15(1) is exhaustive and thus Member States cannot adopt measures for purposes other than those listed.

(iii) Article 15(1) must be interpreted in light of the fundamental rights guaranteed by the Charter and in particular Articles 7, 8 and 11. Any limitation on the exercise of these rights must be subject to the proportionality test articulated in Article 52(1) of the Charter. Measures can only be adopted where it is necessary, appropriate and proportionate within a democratic society in view of the objectives laid down in that provision and they must be strictly proportionate to the intended purpose.

Retention

3.33 The ECJ noted that the Swedish legislation at issue provided for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. It imposed on service providers an obligation to retain that data systematically and continuously, with no exceptions.

3.34 The ECJ referred back to its judgment in *Digital Rights* when noting the far-reaching interference with fundamental rights that the retention of communications and traffic data can entail. It repeated that only the objective of fighting serious crime was capable of justifying such measures. The ECJ went on to state that the general interest objective of fighting serious crime, even if the effectiveness of such depends on the use of modern investigation techniques, could not in itself justify national legislation that provided for the general and indiscriminate retention of all traffic and location data. This far-reaching interference was not necessary for the purpose of that fight and the effect of such legislation would make the retention of data the rule rather than the exception, contrary to what was required by the 2002 Directive.

3.35 Again referring to *Digital Rights*, the ECJ held that such legislation would have the effect of covering all subscribers and registered users and all means of electronic

communication. It provided for no differentiation, limitation or exception according to the objective pursued. It affected all persons using electronic communication services even where there was no evidence to suggest that their conduct might have a link, however indirect or remote, with serious criminal offences. The legislation did not require there to be any relationship between the retained data and a threat to public security and it was not restricted to the retention of data pertaining to a particular time period, geographic area or group of persons etc.

3.36 This type of legislation exceeds the limits of what is strictly necessary and cannot be considered justified within a democratic society. However, the ECJ stated that Article 15(1) does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data for the purpose of fighting serious crime. This is subject to the proviso that the retention of data is limited to what is strictly necessary with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted.

3.37 The ECJ ruled that the following conditions must be satisfied for such legislation to be justified:-

(i) The legislation must lay down clear and precise rules governing the scope and application of a data retention measure.

(ii) The legislation must impose minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse.

(iii) The legislation must indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, so as to ensure that the measure is limited to what is strictly necessary.

(iv) Retention measures must meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, the conditions laid down in the legislation must be shown actually to circumscribe, in practice, the extent of that measure.

(v) The legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal at least an indirect link 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. Examples of such limits include a geographical criterion: where the national authorities consider, on the basis of objective evidence, that there exists in a particular geographical area a high risk of criminality.

Access

3.38 The ECJ reiterated that legislation allowing access to retained data must be proportionate to the seriousness of the interference with fundamental rights that access entails. As such, only the objective of fighting serious crime is capable of justifying such access. The legislation must be proportionate and access must not exceed the limits of what is strictly necessary. The ECJ confirmed in *Ministerio Fiscal* that while a serious interference can only be justified by the objective of fighting 'serious' crime, a less serious interference can be justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally (paras. 56-57).

3.39 The ECJ elaborated as follows:-

(i) Legislative measures must be subject to adequate safeguards. Thus they must lay down clear and precise rules indicating in what circumstances and under what conditions the providers of electronic communications services have to

grant the competent national authorities access to the data. Such measures need to be legally binding. To ensure that the access is limited to what is strictly necessary, national legislation must also lay down the substantive and procedural conditions governing access by the competent national authorities to the retained data.

(ii) General access to all retained data, regardless of whether there is even an indirect link with the intended purpose, cannot be regarded as limited to what is strictly necessary. Therefore, the national legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data. Access can only be granted 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. Access to the data of other persons may also be justified where there is objective evidence that the data might, in a specific case, make an effective contribution to combating such activities.

(iii) It is essential that access should as a general rule, except in cases of validly established emergency, be subject to prior review carried out either by a court or by an independent administrative body.

(iv) A person whose data has been accessed must be notified as soon as that notification is no longer liable to jeopardise any investigations. That notification is necessary to enable the persons affected to exercise, *inter alia*, their right to a legal remedy.

(v) National legislation must make provision for the data to be retained within the EU and for the irreversible destruction of the data at the end of the data retention period. Member States are required also to ensure review by an

independent authority of compliance with the level of protection guaranteed by EU law.

3.40 The ECJ held that it is the task of the national court to determine whether and to what extent the national legislation at issue satisfies the requirements stemming from Article 15(1) read in light of the Charter as set out by the Court.

Conclusion of the ECJ

3.41 In answer to the questions raised by the national courts, the ECJ found that Article 15(1), read in light of the Charter, precludes:-

(i) National legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication; and

(ii) National legislation governing access to the retained data where:

a. The objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime;

b. Access is not subject to prior review by a court or an independent administrative authority, and

c. There is no requirement that the data concerned should be retained within the EU.

<u>The 2011 Act falling within the scope of EU law</u>

3.42 The 2011 Act gave effect to the 2006 Directive. Once the 2006 Directive was declared invalid in *Digital Rights* there was a question as to whether national laws providing

for the retention of data and access to that data by police and security authorities fell within the scope of EU law. This was answered by the ECJ in *Tele2*, as discussed above.

3.43 The Defendants argue that the 2011 Act does not entirely fall within the scope of EU law because it allows for the access of retained data for the purposes of "*the safeguarding of the security of the State*" and "*the saving of human life*" (s. 6(1)(b) and (c)), in addition to "*the prevention, detention, investigation or prosecution of a serious offence*" (s. 6(1)(a)) as was required by the 2006 Directive. The Defendants claim that the two former purposes are areas that fall outside the scope of EU law. Under Article 4(2) TEU national security remains a matter of exclusive Member State competence.

3.44 Although Article 15(1) of the 2002 Directive refers to national security as one of the justifications for restricting the scope of the rights and obligations otherwise provided for in the 2002 Directive, the question about whether measures taken for the purposes of protecting national security fall within the scope of EU law remains live. This question is the subject of a preliminary reference by the IPT. The Plaintiff only seeks a declaration that s. 6(1)(a) is incompatible with EU law and in view of the uncertainty in this area, this Court will restrict any declarations to that section. It may be for another court to determine the applicability of EU law to national security measures.

<u>Retention of data</u>

3.45 The parties disagree as to the correct interpretation and application of para. 112 of *Tele2* which states:-

> "*… Article 15(1) of* [the 2002 Directive], *read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate*

retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."

3.46 Counsel for the Plaintiff stress that para. 112 was "*the beginning, middle and end of the case*" and that it was manifestly clear that the ECJ precluded legislation which permits general and indiscriminate retention and that the 2011 Act provides for this retention. The Plaintiff also relies on the conclusions in the Murray Review which stated at para. 270 that "[t]*here is no longer an obligation on Member States to make provision for a system of communications data retention but if they choose to do so it can only be done by way of an exceptional targeted measure*."

3.47 Four main points were advanced by Counsel for the Defendants:

(i) There should be a narrow interpretation of *Tele2*;

(ii) The reasoning in *Tele2* was not complete;

(iii) The definition of "*general and indiscriminate*" by the ECJ allows for the retention required by the 2011 Act;

(iv) There is a significant difference between the Swedish law and the 2011 Act because the Swedish law provided for access in all criminal activity whereas the 2011 Act was proportionate when it limited its provisions to "*serious crime*".

<u>Defendants' Principal Submissions on Retention in EU Law</u>

"Least Intrusive Means"/A narrow approach

3.48 The Defendants urge this Court to interpret *Tele2* narrowly such that it does not preclude a general retention regime of the kind provided for under the 2011 Act where the objective evidence confirms that this regime is the least intrusive means of interfering with fundamental rights which is capable of achieving the objective of fighting serious crime.

They argue that it is for the Member States to determine, by reference to objective evidence, the 'public' whose data is likely to reveal a direct or indirect link to serious criminal offences and whose data will contribute to fighting serious crime. Accordingly, where a Member State comes to the view that targeted retention will not achieve the objective, then it is entitled to determine that 'public' encompasses the 'entire public using telecommunications services'. They contend that the ECJ reached its decision on the assumption that the objective of Article 15 of the 2002 Directive could be met by "*targeted retention*" and that it did not have any evidence that such retention could be operated effectively. The Defendants contend further that not only would a targeted retention regime be unworkable but it would be "*deeply problematic*" also.

3.49 The Defendants submit that the Advocate General's Opinion in *Ministerio Fiscal*, and by implication the ECJ judgment delivered in October 2018 which agreed with the Opinion, should prompt this Court to adopt a narrow interpretation of *Tele2*. The Defendants argue that the ECJ has narrowly interpreted its judgments in *Digital Rights* and *Tele2* when it determined that access to retained data is not confined to cases in which the offence concerned is of a serious nature (as was suggested in *Tele2*) where the interference with rights is not particularly serious.

3.50 Furthermore, any conclusion by this Court, according to the Defendants, that the ECJ in *Tele2* has prohibited general and indiscriminate retention is a radical development on the part of the ECJ after its restraint shown earlier in *Digital Rights* in not going that far.

Conclusion on a narrow approach

3.51 The position of the Defendants is difficult to reconcile with the conclusions of the ECJ which clearly state that the objective of fighting serious crime cannot in itself justify legislation providing for general and indiscriminate retention of data. In order for the

legislation to be considered strictly necessary, it must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal at least an indirect link 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. Interpreting 'public' as 'the entire public using telecommunications services' defeats the purpose of *Tele2* and disregards the ECJ's conclusions that a general and indiscriminate retention regime is a far-reaching interference with fundamental rights. It also makes the retention of data the rule rather than the exception.

3.52 While *Ministerio Fiscal* was the first occasion on which the ECJ had been called to interpret its earlier judgment in *Tele2*, it is still not possible to read something into *Tele2* which detracts from the clear wording of para. 112 that precludes general and indiscriminate retention. It should also be noted that the ECJ in *Ministerio Fiscal* was only concerned with the conditions governing the access by national authorities to personal data in the electronic communications sector and not to the retention of such data. It was assumed that the data had been retained in accordance with the national legislation and in compliance with the conditions laid down in Article 15(1) of the 2002 Directive. *Ministerio Fiscal* cannot therefore be interpreted as refining the conditions for retention.

3.53 Although "*targeted retention*" is mentioned in *Tele2*, it is not the case that the ECJ did not consider anything other than targeted retention. Ireland's written observations to the ECJ, dated 21st August, 2015 (referred to in the preamble to *Tele2*), discussed the difficulties with targeted retention. For example para. 26 of the observations stressed that it was "*simply not possible to identify the individuals, locations or dates relevant to an investigation in advance or at the outset of the investigation*". However much the Defendants may not agree with the conclusions of the ECJ and argue that a targeted regime is not feasible in practice, it is not open to this Court to distort these conclusions such as to render them meaningless.

3.54 In the opening and on other occasions, Mr. Farrell SC for the Plaintiff repeated his suggestion that the Defendants showed a desire to re-litigate aspects of *Digital Rights* and *Tele2*. After having been furnished during the hearing with Ireland's written observations Mr. Farrell rhetorically and pointedly asked:-

> "*How can it be the case that a Member State is entitled to make sophisticated, clear, cogent arguments before the CJEU* [and] *by clear implications have those arguments rejected and then come back before the courts of the Member States and effectively try the same argument again?*"

3.55 Mr. Farrell with conspicuous ability accepted that "*it would be extremely difficult to resist a request by the State defendants for a reference to the CJEU if they contended that the CJEU had not engaged with the arguments of the State*" about the interaction between Article 1(3) and Article 15(1) of the 2002 Directive. The Defendants sought to persuade this Court that a reference was not required while recognising that this Court of its own volition could refer a question. The circumstances of fact and law do not merit a reference.

Indiscriminate

3.56 There was also debate in this Court about whether the word "*indiscriminate*" merely requires the absence of objective justification in the drafting of the legislation in contrast to the implementation of the legislation. The Defendants pointed to the choice of two years for telephony data in the 2011 Act and one year for internet communications. The Defendants highlighted that the word "*indiscriminate*" was not used at all by the Advocate General in *Tele2* and that there is some significance to the fact that the ECJ departed from the Advocate General's description of a general data retention obligation. They argued that "*general and indiscriminate*" can be interpreted in two ways:-

(i) As a single phrase with a single definition meaning retention which is general and applies to everyone without distinction; or

(ii) "*General and indiscriminate*" with two separate meanings:- "*General*" means that the retention applies to everyone but "*indiscriminate*" refers to retention that is ill-considered, arbitrary and lacking in objective justification. In this way, the Defendants claimed that the 2011 Act does not fall foul of "*indiscriminate*" because it is general for a good, objective and justifiable reason. It is submitted that the 2011 Act regime achieves an objective and is thus not indiscriminate.

Conclusion on "general and indiscriminate"

3.57 The phrase "*general and indiscriminate*" is clear. It is true that the phrase does not appear in the opinion of the Advocate General in *Tele2* and the question referred to the ECJ by the Swedish Court refers to a "*general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data* ***without any distinctions, limitation or exceptions*** *for the purpose of combatting crime*" (para. 51, emphasis added).

3.58 This phrase comes from the report dated 13th June, 2014, of a special reporter appointed by the Swedish Minister for Justice to examine the Swedish legislation in light of *Digital Rights*. The ECJ noted that "*the special reporter emphasised that the* Digital Rights *judgment could not be interpreted as meaning that the* ***general and indiscriminate retention of data*** *was to be condemned as a matter of principle*" (para. 46, emphasis added).

3.59 Is there any significance in the use by the ECJ of "*general and indiscriminate*" as opposed to "*without any distinctions, limitations or exceptions*"? I cannot identify any such significance.

3.60 While the Defendants asked this Court not to become "*over-fixated*" in the use of language, it is possible for the Court to consider the other language versions of *Tele2*. The languages used in the judgment were English and Swedish which have equal authority (as per Article 41 of the Rules of Procedure of the Court of Justice). In the Swedish version, the word is "*odifferentierad*" which translates as "*undifferentiated*". In those circumstances, it is not apparent how the use of the English word "*indiscriminate*" could be interpreted as meaning "*arbitrary or lacking an objective justification*" rather than the ordinary meaning of unrestricted and general.

Differences in legislation – 2011 Act compared with Swedish/UK laws

3.61 The Defendants further focus this Court's attention on differences in detail between the Swedish legislation examined in *Tele2* and the 2011 Act. In other words, the Defendants, while disavowing an intention to request or suggest a reference to the ECJ, argue before this Court that there are such differences in the various national laws as to require this Court to modify the ordinary meaning of the words used by the ECJ in *Tele2*.

3.62 Considering *Tele2*, this argument is not convincing. Throughout the judgment the ECJ referred to 'serious crime' and specifically stated that "*only the objective of fighting serious crime is capable of justifying such a measure*" (para. 102). The absence of a reference to "*serious crime*" in the Swedish legislation in *Tele2* is not a particularly distinguishing factor which this Court is prepared to accept in this context.

<u>Overall Conclusion</u>

3.63 The ECJ in *Tele2* is unequivocal about the necessity for clear and precise rules in relation to data retention (see especially paras. 107-109). As such, the primacy of EU law, the ECJ's consideration of submissions made by various Member States and notably those of

Ireland before *Digital Rights* and *Tele2*, together with the submission of Mr. Farrell SC against re-litigating without a request for a reference to the ECJ have persuaded this Court that such part of s. 3 of the 2011 Act which requires all service providers to retain the telephony data for two years is indeed general and indiscriminate. In addition, it is not possible to identify that the ECJ has limited its prohibition against general and indiscriminate retention to the application of legislation as opposed to the enactment of legislation.

3.64 One cannot perhaps be more succinct in explaining the effect of *Tele2* than by quoting the summary of the impact of the judgment and particularly the following from para. 12 of the Murray Review:-

> "*The* [ECJ] *held that the existing forms of automatic and wholly indiscriminate retention of private communications data cannot be reconciled with European law. It concluded that retention can only occur, exceptionally, in pursuit of the objectives which are exhaustively listed in Article 15(1) of* [the 2002 Directive], *and cannot be wholly indiscriminate without exception, in scope and application.*"

<u>If *Tele2* did not affect the 2011 Act?</u>

3.65 The principal aim of the Defendants' arguments was to persuade this Court to do its own proportionality assessment on the 2011 Act based on the evidence adduced before this Court.

3.66 Considering what might have been just because this is a court of first instance ought not be undertaken. Assessing the evidence about the necessity and proportionality of s. 3 for the general and indiscriminate retention of telephony data for the 407 phone against the EU law governing surveillance and privacy without regard to *Tele2* does not permit this Court to modify the meaning of *Tele2*.

3.67 One of the biggest difficulties for this abstract scenario, if it were to be pursued, could be the pinning down of the month or year during which that exercise is to be fulfilled. The above summary of the evidence before this Court could lead to a conclusion that the retention of the telephony data for the 407 phone was very useful if not crucial to the investigation into the disappearance of the Victim and the later successful prosecution of the Plaintiff. However, I specifically decline to make any such finding because it falls outside what can be decided now. As desirable as it may appear for this Court to answer all questions including hypothetical ones, other courts to which the parties have access can determine the essential questions which follow from the conclusions of this Court.

Retention under ECHR

3.68 The Plaintiff also seeks a declaration under s. 5 of the ECHR Act that the retention of data pursuant to s. 3 of the 2011 Act was general and indiscriminate and as such contravened Articles 8 and 10 of the ECHR.

Preliminary issue

3.69 Section 5 of the ECHR Act provides that the Court may "… *where no other legal remedy is adequate and available, make a declaration … that a statutory provision or rule of law is incompatible with the State's obligations under the Convention provisions*." The Supreme Court in *Carmody* determined that the remedy provided by s. 5 of the ECHR Act is "*both limited and* sui generis [and] *does not accord to a plaintiff any direct or enforceable judicial remedy*." (para. 41).

3.70 Even if the declaration that the Court will make about inconsistency with EU law concerning retention is enough for the Plaintiff, the Court will, for the sake of completeness, now consider the arguments relying upon the ECHR.

Retention

3.71 Article 8 of the ECHR protects the right to respect for private and family life:-

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

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

3.72 The ECtHR has made no clear pronouncements on the validity or not of a general and indiscriminate data retention regime. Even in the context of bulk interception regimes concerning the content of communications, the ECtHR has iterated that these regimes *per se* fall within the wide margin of appreciation that national authorities enjoy when choosing how best to achieve the legitimate aim of protecting national security (*Big Brother Watch* para. 314). The ECtHR has focussed its attention on the necessity of safeguards to minimise the risk of abuses of power.

3.73 The separate but concurring opinion of Judges Yudkivska and Bošnjak in *Benedik* makes it clear that the ECtHR has not recognised that in the digital age it may be no longer accurate to define the interception of the content of communications as a greater interference than the interception of metadata (as discussed in *Malone v. U.K.*, 2nd August, 1984, Series A, No. 82). The Judges stated that this case "*presented a unique opportunity to clarify the scope of the reasonable expectation of privacy in the digital age*" (p. 45).

3.74 In *Big Brother Watch*, the ECtHR noted that in their previous case of *Ben Faiza v. France*, (App. No. 31446/12, 8th February, 2018), (**"*Ben Faiza*"**) it "*distinguished between methods of investigation which made it possible to identify the past geographical position of*

a person and those which made it possible to geolocate him or her in real time, indicating that the latter was more likely to violate the right to respect for private life." (para. 462). The ECtHR concluded that "*the transmission to a judicial authority of existing data held by a public or private body was to be distinguished from the establishment of a surveillance system, such as the ongoing monitoring of a telephone line or the placing of a tracking device on a vehicle*" (para. 462).

3.75 The question as to whether or not a general and indiscriminate retention regime is compatible with the ECHR remains undetermined. It is not for this Court to go further than the ECtHR. In *McD v. L* [2010] 2 I.R. 199, in the context of an interpretation under s. 2 of the ECHR Act, Fennelly J. quoted with approval Lord Bingham in *R (Ullah) v. Special Adjudicator* [2004] 2 A.C. 323 who warned against going further than the ECtHR:-

> "*In determining the present question, the House is required by Section 2(1) of the Human Rights Act, 1998 to take into account any relevant Strasbourg case law. While such case law is not strictly binding, it has been held that courts should, in the absence of some special circumstances, follow any clear and constant jurisprudence of the Strasbourg court … This reflects the fact that the Convention is an international instrument, the correct interpretation of which can be authoritatively expounded only by the Strasbourg court. From this it follows that a national court subject to a duty such as that imposed by section 2 should not without strong reason, dilute or weaken the effect of the Strasbourg case law … It is of course open to member states to provide for rights more generous than those guaranteed by the Convention, but such provision should not be the product of interpretation of the Convention by national courts, since the meaning of the Convention should be uniform throughout the States party to it. The duty of national courts is to keep pace*

with the Strasbourg jurisprudence as it evolves over time: no more, but certainly no less." (para. 323).

3.76 Therefore, this Court cannot make a declaration under s. 5 of the ECHR Act that s. 3(1) [retention] is incompatible with the right to respect for private life under Article 8.

Access

Introduction

3.77 Access to the retained data for the 407 phone by investigators to attribute the use of the master and slave phones forms the second basis of the Plaintiff's claim in these proceedings.

Plaintiff's submissions

3.78 The Plaintiff claims that the provisions for accessing the retained data did not meet the requirements of EU, ECHR and constitutional law on the following grounds:-

(i) The 2011 Act in not providing for meaningful conditions governing access and use of the retained data is disproportionate;

(ii) The collation and disclosure of data is not subject to a substantive review by a court or other independent authority that ought to vindicate individual rights;

(iii) The 2011 Act does not provide sufficient safeguards to ensure effective protection of retained data against the risk of abuse or unlawful access of the retained data.

3.79 The Plaintiff claims that safeguards must be set out in enforceable measures of law rather than forms of soft regulation and that all the safeguards set out in paras. 60-68 of *Digital Rights* are mandatory. The Plaintiff also relies on the Murray Review where it recommended that "*the detailed rules governing data security to which the ECJ alluded,*

together with the obligations imposed on Service Providers in this regard, should be incorporated into the enactment establishing a data retention and disclosure scheme." (para. 267). Further, the Review stated that Member States are required to ensure that service providers take appropriate technical and organisational measures in order to guarantee a particularly high level of protection and security against unlawful access and that this "*can only be effectively done by enumerating the security standards and procedures with which Service Providers are obliged to comply in national legislation*." (para. 272).

3.80 In addition, the Plaintiff argues that the practice regarding access under the 2011 Act, i.e. the activities of the TLU, consists of self-certification by the Gardaí, as discussed in para. 256 of the Murray Review. The Review found that currently there is no form of prior independent authorisation and that "*this arrangement is no longer tenable*" following *Tele2* (para. 386). The Plaintiff also states that regard can be had to the ECtHR's case law to define an 'independent administrative authority', as per Article 52(3) of the Charter.

Defendants' submissions

3.81 The Defendants argue that the 2011 Act contains important substantive and procedural conditions governing access and use of retained data and that the regime established under the Act provides for prior independent review of disclosure requests. The Defendants claim that the TLU is independent of the investigative teams. They may make disclosure requests and the TLU verifies the legality, proportionality and necessity of all disclosure requests sought by a member of the Gardaí. Furthermore, this review is combined with a system of independent judicial and regulatory oversight by the designated judge.

3.82 They referred to:-

(i) The manner by which the TLU operated with the assessments of disclosure requests during the investigation leading to the Plaintiff's trial and conviction;

(ii) The audit and supervision provided by the DPC and the independent judge respectively over the years;

(iii) The lack of any specific requirement for prior judicial review of access requests in other areas of criminal law and investigations. The Defendants mentioned the judgment of Charleton J. in *CRH Plc, Irish Cement Ltd v. Competition and Consumer Protection Commission* [2018] 1 I.R. 521 in their submissions on the constitutional issue but it nevertheless resonates here. In para. 246 Charleton J. pointedly contrasted how contemporary law protects the right of privacy in the context of searches:-

> "*Resort to a private space, it must also be recognised, may be for illegal and even criminal purposes. There are some spaces into which the law has no entitlement to intrude, even though it may disapprove of actions which in themselves are an aspect of human expression; see the dissenting judgment of Henchy J. in* Norris v. Ireland *[1984] I.R. 36 at pp. 71 and 72. Circumstances may dictate where a right to privacy may be asserted, as where a couple converse in their own bedroom, and where the assertion of such a right is not to be met with favour, as where people meet in a public forum, and this is recorded as a fact, or engage with newspapers or television or the internet as to their life or opinions in such a way as to make themselves an aspect of wide interest. The nature of the conduct may also have a bearing on whether any right to be left alone is engaged. Criminal conduct is not planned publicly and nor do conspirators generally give advance notice of their actions. Hence, to organise a crime, resort is had to what may be otherwise described as the private*

> *space. The Constitution, in contemplating the attainment of "true social order", as recognised in the Preamble, could hardly extend to the planning of crime the protection of a specific right that is recognised because of the legitimacy of people being enabled to retreat from public notice. That there may be legal rights attached to communications through telecommunications is undoubted, legislation provides for this, and their general application is necessitated by the need to protect the public. But, there is no constitutional right of privacy that inures to the organisation of a crime*."

3.83 Furthermore, the Defendants argue that the ECJ did not explain what was meant by an independent administrative body or authority. Thus, this matter is for the national court to decide on the basis of the Irish provisions and the evidence presented.

3.84 The Defendants submit that the ECJ in both *Digital Rights* and *Tele2* did not use the language of Article 47 of the Charter and Article 6 ECHR which refer to '*an independent and impartial tribunal … established by law*'. Thus, the Defendants effectively argue that something different was clearly envisaged.

3.85 The Defendants acknowledge that the ECJ in *Tele2* approved the analysis of the ECtHR in *Szabo and Vissy v. Hungary* (2016) 63 E.H.R.R. 3 where it held that:-

> "*… the rule of law implies,* inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*." (para. 77).

3.86 However, the Defendants argue, first, that the ECtHR has stated that the intervention of judicial authority in authorising access is not mandated by the Convention. Second, in seeking independent authorisation, the concern was that there be independence from executive interference to avoid the risk of political influence over the authorisation process and third, the requirement of *ex ante* authorisation is not absolute as long as there is extensive *ex post facto* judicial oversight which might counterbalance the shortcomings of the authorisation.

3.87 The Defendants argue that the system put in place by the 2011 Act meets these requirements in that the TLU is independent of the investigation, it is the 'body' or 'authority' which administers applications under the Act and there is judicial oversight through the designated judge, a complaints procedure, judicial review and judicial supervision where the material is relied upon in the course of a criminal trial.

The Access Regime operated by the Gardaí – Overview

3.88 DCS Peter Kirwan in his twenty-page statement and his evidence given on days 5, 6 and 8 of the hearing before this Court was forthcoming in giving the facts that allow the Court to give an overview of the access system which operated with and without specific statutory provisions in 2012 and 2013:-

(i) Any garda could request access to retained telephony data;

(ii) The Gardaí set up the TLU without a specific statutory requirement to do so. The TLU has staff dedicated to performing the exclusive function as the single point of contact for administrating requests for data from the Gardaí to the communications service providers such as Vodafone;

(iii) DCS Kirwan was the garda officer directly responsible for the TLU at the time of the request for the 407 phone;

(iv) An Assistant Commissioner was the "*immediate boss*" of DCS Kirwan;

(v) DCS Kirwan engaged with the "*oversight judge*" who performed specific duties under s. 12 of the 2011 Act and the DPC acted as the national and supervisory authority for the 2011 Act and the 2006 Directive, under s. 4(2) of the 2011 Act;

(vi) DCS Kirwan could have taken requests for access equally from more senior officers than himself in the Gardaí;

(vii) DCS Kirwan had some familiarity with the facts surrounding the disappearance of the Victim prior to the first request for access to the 407 phone because of applications for retained data of other phones as may be gleaned from the chronology earlier in this judgment. The investigating team based at Blackrock Garda Station first applied for subscriber details for the 407 phone on the 30th September, 2013. The team followed that up with four other disclosure requests on the 4th October, 2013, in the format provided by the TLU which accommodated the capabilities of service providers;

(viii) DCS Kirwan explained how he considered each application and how it related to the investigation of a "*serious offence*". He satisfied himself that access was necessary and proportionate in the case of the 407 phone;

(ix) DCS Kirwan exhibited integrity and diligence of a high standard when acceding to applications and making the request for details of the subscriber and retained data for the 407 phone from Vodafone;

(x) DCS Kirwan accepted in cross-examination that filtering results as might be undertaken in the UK statutory equivalent of a TLU to minimise "*collateral intrusion*" into the rights of others was not available in Ireland. Nevertheless the degree to which DCS Kirwan went in investigations to avoid releasing

intrusive information on others was commendable given the limited statutory direction and requirements in that regard.

Efforts by the Gardaí to comply with the ECHR

3.89 The Court in its chronological summary has sought to identify, from the MoU in 2011 to the 2013 Garda HQ Directives, the attempts by An Garda Síochána to facilitate secure access for retained data proportionally. There was no hint from DCS Howard, Conor O'Callaghan, Ms. Skedd or any other witness, despite thorough examination before this Court, that access to retained data was abused in the case of the Plaintiff.

Data Protection Commissioner Audit

3.90 Mention was made at the hearing before this Court of the "*final report of audit*" by the DPC in 2014 relating to procedures to ensure that requests were valid. The evidence from the Gardaí is that the concerns of the DPC have been addressed.

Incident meriting sanction

3.91 During cross-examination DCS Kirwan clarified that the unauthorised use by a garda for personal reasons prior to the 2011 Act of similar provisions for accessing retained data "*was uncovered by internal processes*". The oversight judge referred to this incident in his annual report and DCS Kirwan said, although he was not involved with any of the units at the time, that some disciplinary proceedings had been taken. It is noteworthy that no sanction remains specified for misuse of access under the 2011 Act. Furthermore a subject of misuse of retained data may never discover an actual or potential breach of EU law due to the absence of a provision for notice to a subject in the 2011 Act. The extent of transparency and

supervision is left to the effort of the Gardaí to comply with the necessity, proportionality and appropriateness requirements which are acknowledged to be applicable.

Decision on EU law re access

3.92 The 2002 Directive requires that Member States ensure the confidentiality of communications in accordance with the Charter and ECHR (Recitals 2 and 3 together with Article 5). However there is no specific requirement set out for access to retained data.

3.93 The now invalid 2006 Directive, on the other hand, recognised increasing international demand for national laws to define procedures that ensure access is gained in accordance with necessity and proportionality requirements.

3.94 More significantly, the ECJ in *Digital Rights* identified fatal gaps in the 2006 Directive because it:-

(i) did not lay down any objective criterion by which to determine the limits to be placed on the access and subsequent use of data;

(ii) did not contain substantive and procedural conditions relating to access and use;

(iii) did not provide that access and use be strictly restricted to fighting serious crime;

(iv) did not require that access by the competent national authorities be dependent on a prior review carried out by a court or by an independent administrative body; and

(v) did not require that the data must be retained within the EU.

3.95 The ECJ in *Tele2* clarified that these requirements were mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data. Therefore the provisions of the 2011 Act relating to access fall foul of EU law requirements.

ECHR law and access

3.96 The Plaintiff also claims that the access regime violates his rights under Article 8 of the ECHR. While the ECtHR has considered many cases in the area of data protection the majority of cases concern mass surveillance in the context of the content of communications. As such, this Court is cautious in transferring the principles outlined in these cases to cases involving telephony metadata especially as the ECtHR has so far seemed disinclined to do so. In cases involving legislative measures concerning the fight against crime and terrorism, the ECtHR has accorded a significant margin of appreciation to States.

3.97 The ECtHR, in considering whether an interference is justified under Article 8, asks whether the legislative measures is in accordance with law. The measure must:-

(i) have some basis in domestic law;

(ii) be accessible to the person concerned;

(iii) be foreseeable as to its effects; and

(iv) be compatible with the rule of law, i.e. it must provide adequate protection against arbitrary interference (see for example *Benedik* para. 122, where the Slovenian authorities had sought access to subscriber information associated with a dynamic IP address under a provision of Slovenian law).

3.98 The ECtHR has held that it must thus:-

"*be satisfied also that there are adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law*" (*Benedik* para. 125).

3.99 Where State actions are undertaken in secret there must be adequate and effective safeguards against arbitrary interference. The ECtHR has stated there is a risk that a system

of secret surveillance may undermine or even destroy democracy under the cloak of defending it.

3.100 In *Ben Faiza* the ECtHR considered an order issued pursuant to domestic law to a service provider requiring it to provide lists of incoming and outgoing calls on four mobile telephones as well as the list of cell towers 'pinged' by those telephones. The ECtHR held that the measure was in accordance with law because it contained safeguards against abuse. The issuing of any order must be authorised by the public prosecutor. The Cour de cassation had also held that this authorisation is an absolute requirement and failure to obtain such would invalidate the act. Furthermore, the ECtHR noted that the authorisation was subject to a judicial review in the subsequent criminal process and there is the possibility of evidence being excluded. However, it should be noted that this *ex post facto* judicial control will only be exercised when a criminal prosecution is brought.

3.101 In *Big Brother Watch* the ECtHR considered the regime for the acquisition of communications data under Chapter II of RIPA. The ECtHR found that interference cannot be considered to be 'in accordance with law' if it does not comply with domestic law and that the ECtHR cannot question the interpretation of national courts save in exceptional circumstances. The ECtHR referred to the recent judgments of the UK courts and held that it is clear that "*domestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data by* [service providers] *limits access to the purpose of combatting "serious crime", and that access be subject to prior review by a court or independent administrative body*." (para. 467). As the Chapter II regime failed on both of these issues, the ECtHR held that there was a violation of Article 8.

Conclusion on access

3.102 It is readily apparent, as detailed in the Murray Review at paras. 89-133 and 294-324 in particular, that the Gardaí have sought to grapple with the effects of the ECHR Act from the 2013 Garda HQ Directives to the aftermath of *Digital Rights* in April 2014. Creating the TLU was the only remedial action that the Gardaí could take without legislation in an effort to comply with EU and ECHR law. The deficiencies as identified in the Murray Review compel this Court to agree that "*serious attention should be given to the question of statutory cohesion in the matter of data retention and disclosure*" (para. 310).

3.103 Therefore, the demands of a modern day democratic society to guarantee the fundamental right to privacy prescribed by EU and ECHR law for access to retained telephony data have not been met by the 2011 Act.

3.104 There is the unsatisfactory scenario of the senior garda who handles applications and determines necessity, appropriateness and proportionality with an eye on collateral intrusion, is subordinate to a higher ranking officer. An application for access by a superior who has directed a criminal investigation leading to such a request does not fit with the concept of an independent authority. There is an increasing requirement for prior independent judicial or independent administrative scrutiny and notification to a citizen about a review whether in advance or soon after the obtaining of access.

3.105 No aspersion was cast upon the integrity of the independent judge or the audit-like powers exercised by the DPC under the 2011 Act. However, the whole system under the 2011 Act does not allow for citizens whose retained data and thereby their privacy rights under EU law and ECHR law are trenched upon to learn of that retention and access. The Plaintiff in this case may have known that the telephony data for the 407 phone had been retained and was later accessed at various relevant times. However, that does not affect the application of EU law and the ECHR in Ireland.

3.106 In those circumstances this Court finds that the provisions set out in s. 6(1) of the 2011 Act contravene EU law and the ECHR because there is no prior review by a court or an independent administrative authority for access to the telephony data. In addition, there are no adequate legislative guarantees against abuse. Too much is left to those who implement and utilise the access provisions.

4. REMEDIES

Introduction

4.1 It now remains for the Court to consider the terms of the declarations which are the only reliefs sought. Furthermore, the arguments about the temporal effect of the declarations require a decision on whether they should only have effect from a particular date or be suspended for a period of time.

Content of Declarations

4.2 As discussed at paras. 1.18-1.19 and 3.44, the Court has identified that any declarations which can be made do not concern "*the safeguarding of the security of the State*" or the "*saving of human life*".

4.3 Although the Court is more aware now about the ever-increasing communications over the internet, the Court concentrates on telephony data. The Plaintiff only seeks a declaration which could be relevant to the admissibility of the telephony data for the 407 phone. Other litigants and courts may raise points about internet communications which have not been considered here. Therefore, the declaratory reliefs should be confined to telephony data.

4.4 The Plaintiff argues that the definition of 'serious crime' under the 2011 Act is so broad as to encompass the majority of offences. However, murder is undoubtedly a serious

crime. The Plaintiff has no standing to rely on the suggestion that 90% of indictable crimes fall within the definition of "*serious offence*" (s. 1 of the 2011 Act). It is neither necessary nor practicable to carve out a separate declaration to cover potential offences which might fall foul of the EU law requirement for a "*serious offence*" in a further application of the proportionality principle as mentioned in *Ministerio Fiscal*.

Temporal Issues

4.5 An "*invalid*" document or law is not legally or officially acceptable. Counsel, without prejudice to other submissions agreed in July, 2018, that the Defendants should proceed first in their submissions about the jurisdiction of this Court to impose some temporal restrictions due to the common law presumption of retrospective effect of declarations relating to the validity of legislation under the Constitution.

4.6 Counsel for the Plaintiff likened the way by which the Defendants wanted the Court to assess the effect of invalidity to Schrödinger's cat thought experiment. The position of the Defendants at various points in the chronology merits a recap to contextualize the dilemmas which occurred:-

(i) the unsuccessful challenge of Ireland to the 2006 Directive, *Ireland v. Parliament*, that resulted in the ECJ finding (9th February, 2009) the 2006 Directive to be "*essentially limited to service providers*" and advising *inter alia* the State itself was not retaining the data;

(ii) the declaration of the ECJ (26th November, 2009) that Ireland had failed in its obligation to implement the 2006 Directive which required the Oireachtas to enact legislation, *Commission v. Ireland*;

(iii) the finding of the ECJ in *Digital Rights* (8th April, 2014) that the 2006 Directive "*is invalid*" on the ground that the EU legislature had not complied

with the principle of proportionality "*in the light of Articles 7, 8 and 52(1) of the Charter*", necessitated an appraisal of the reliance by the State on the derogation in the 2002 Directive for the obligation of service providers to retain data;

(iv) the interpretation by the ECJ in *Tele2*, (21st December, 2016) of a clear prohibition of "*general and indiscriminate retention of all traffic and location data*" and the imposition for access of "*prior review by a court or an independent administrative authority*" albeit in references to the ECJ from other Member States, ought to have increased concern in Ireland about the 2011 Act;

(v) the recent reinforcing judgments of the ECtHR about the necessary safeguards for access to retained data cannot be ignored by Ireland; and

(vi) the stark conclusions of the Murray Review about retention and access under the 2011 Act which was presented in April 2017 and which prompted the ongoing legislative process to amend the 2011 Act.

4.7 A declaration of incompatibility with EU law, while merely declaratory relief, creates an obligation on courts to disapply that law in relevant cases. The Defendants acknowledge that to the extent that the 2011 Act is inconsistent with EU law, the organs of the State would be bound to disapply the 2011 Act (*Simmenthal*). However, the Defendants argue, firstly, that the effects of such a declaration should be prospective only; secondly, the effects of such a declaration should be suspended in order to give the Oireachtas an opportunity to amend the legislation.

Prospective effect

4.8 The following uncontroversial propositions concerning the effects of a declaration of invalidity can be listed:-

(i) It is for the courts of Member States "*to draw the consequences in their legal system of the declaration of invalidity*" made in a reference for preliminary rulings under Article 267 TFEU (see *Rey Soda v. Cassa Conguaglio Zucchero (Case 23/75)* [1975] E.C.R. 1279, para. 51). Therefore, any question about the validity of national legislation implementing or otherwise falling within the scope of EU law is a matter for the national courts applying EU Law, as reiterated by the ECJ in *Tele2*, para. 124.

(ii) The ECJ has exclusive jurisdiction only in determining the validity of EU legislation which applies across all Member States. The ECJ in *Schrems* (*Case C-362/14)* ECLI:EU:C:2015:650) at para. 61 confirmed that the exclusivity of that jurisdiction has "*the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly*".

(iii) Due to the fact that there is no common legislative framework at EU level for dealing with declarations of invalidity of EU law each Member State is informed by its own national rules when considering legislative measures providing for the retention of telephony data in accordance with Article 15(1) of the 2002 Directive.

(iv) The ECJ did not impose a temporal restriction on its declaration of invalidity of the 2006 Directive.

(v) The possibility of temporally limiting the effects of a declaration of invalidity of a direct action is provided for under Article 264 TFEU and the ECJ has applied this by analogy to preliminary rulings under Article 267 TFEU (*Volker*

und Markus Schecke GbR and Hartmut Eifert v. Land Hessen (Case C-92/09) [2010] I-11063, para. 93)

(vi) A national court is not precluded from drawing guidance from the approach of the ECJ in addition to relying on its own body of law when considering whether the effects of a declaration of invalidity are applied *ex nunc* or *ex tunc*. See for example the judgments of Henchy J. and Kenny J. in *Murphy v. Attorney General* [1982] I.R. 241 (***"Murphy v. AG"***) where they cited *Defrenne v. Sabena (Case C-43/75)* [1976] E.C.R. 445 (***"Defrenne"***).

Defendants' Submissions

4.9 While reserving the right of the State to re-argue in the Supreme Court the law outlined in *Murphy v. AG*, that a declaration of invalidity of a law having regard to the provisions of the Constitution (Article 34.3.2˚) renders an Act void *ab initio*, the Defendants submit that there is no such absolute rule of retrospectivity when applying EU law at a national level. This Court was requested to adopt the ECJ's approach, albeit in exceptional circumstances, to limit the temporal effect in the interest of legal certainty and to take account of the serious effects which the declarations may have.

4.10 The following principles were extrapolated and emphasised from the ECJ case law when imposing a temporal limitation:-

(i) there must have been legitimate uncertainty as to whether the law was valid;

(ii) Member States must have legitimately relied on the validity of the law;

(iii) a significant disruption to the public interest can displace the usual retrospective effect of a declaration of invalidity;

(iv) encouragement from community institutions to Member States leading them to believe that the law was valid can be taken into account; and

(v) legal certainty is required for society to work properly.

(See cases: *Defrenne*; *Barber v. Guardian Royal Exchange Assurance Group (Case C-262/88)* [1990] E.C.R. I-1889; *Wienand Meilicke and Others v. Finanzamt Bonn-Innenstadt Case C-292/04* [2007] E.C.R. I-1835; *Banca populare di Cremona Soc. coop. arl v. Agenzia Entrate Ufficio Cremona (Case C-475/03)* [2006] I-9373; *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen (Case C-92/09)* [2010] E.C.R. I-11063).

4.11 According to the Defendants, this Court is entitled to have regard to the unique circumstances arising in this case:-

(i) The entire 2006 Directive was struck down by the ECJ eight years after coming into effect and after it had become embedded in the legal systems of the Member States. The declaration of invalidity for the 2006 Directive is the first time where legislation had been in force pursuant to a Directive for a number of years before the finding of invalidity of the underlying Directive. The Defendants clarified that there were other Directives and Regulations annulled for procedural or substantive reasons but the 2011 Act stands out as legislation which had become embedded in the legal systems of Member States for years prior to the declaration of invalidity in *Digital Rights*.

(ii) The Defendants state that there is very considerable reliance being placed on the validity of those laws in a fundamental aspect of our society, namely in the investigation and collection of evidence in relation to the running of criminal trials. Thus, invalidating the 2011 Act would be a very significant step with regard to its effects and would involve a significant disruption of the expectations legitimately based on the law as it stood.

(iii) The Defendants argue that up until 8th April, 2014, Member States were under an obligation of EU law to give effect to the 2006 Directive.

(iv) On only one other occasion has Ireland had to amend legislation by reason of a declaration of invalidity for a Directive pursuant to which the legislation was enacted. In *Association Belge des Consommateurs Test-Achats and Others (Case C-236/09)* [2011] E.C.R. I-773, the ECJ ruled that insurers could no longer take sex into account when calculating insurance premia notwithstanding the rule laid down in a Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services. The ECJ delayed the entry into force of that judgment until the expiry of an "*appropriate transitional period*" which allowed insurance companies time to adjust to the ruling. Subsequent to that ECJ judgment, the Equal Status (Amendment) Act 2012 was enacted.

4.12 Therefore, the Defendants argue that there are overriding considerations of legal certainty in this case and as such the effect of any declaration of inconsistency with EU law is that the 2011 Act should be disapplied from the date of declaration.

Decision on prospective effect

4.13 With regard to temporal limitations, as noted above, the national court should first and foremost follow its national procedural rules. Where there has been a breach of constitutional rights the courts will seek to grant a remedy. It was stated in *Carmody* that the "*court is one of the organs of government*" and "[i]*n exercising its judicial functions it must seek to vindicate*" constitutional rights (paras. 122-123). Only in exceptional circumstances should the Court decline to grant a remedy for a breach of rights, be it constitutional or EU. Henchy J. in *Murphy v. AG* under Part VII at pp. 313-314 with remarkable clarity and foresight

explained these matters which were encapsulated then in the following sentences in the judgment of Griffin J.:-

> *"When a statute has been declared to be void* ab initio*, it does not necessarily follow that what was done under and in pursuance of the condemned law will give to a person, who has in consequence suffered loss, a good cause of action in respect thereof. Notwithstanding the invalidity of the statute under which such act was done, the Courts recognise the reality of the situation which arises in such cases, and that it may not be possible to undo what was done under the invalid statute – as it was put so succinctly during the argument, "the egg cannot be unscrambled.""* (p. 331).

4.14 The Defendants' argument essentially amounts to a plea not to 'unscramble the egg' because invalidating the 2011 Act will involve a significant disruption of the expectations legitimately based on the law as it stood. There are, however, several distinguishing features of the case before this Court and the facts in *Murphy v. AG*. In *Murphy v. AG*, the consequences of the declaration of unconstitutionality were clear – potentially tens of thousands of people could claim compensation from the State, causing great economic uncertainty (Henchy J., p. 317). There were no other hurdles which potential plaintiffs would be required to surmount. However, in this case, it is not an automatic consequence that trials will collapse or that convictions will be quashed. The Plaintiff, and others, will be obliged to address the rules regarding the admissibility of evidence. This Court, as opposed to the Court of Appeal, to which the Plaintiff has appealed his conviction, is only seized with the claim for declarations. The rules of evidence which stemmed from *DPP v. Kenny* and revised by the majority of the Supreme Court in *J.C.* as may be applied to the Plaintiff's appeal are not for this Court's consideration.

4.15 The following comparison of the Plaintiff's case with another scenario may elucidate how unscrambling the egg can be done differently and can have different consequences. The

claim before this Court can be distinguished from that in *In re Haughey* [1971] 1 I.R. 217 where the Supreme Court declared s. 3(4) of the Committee of Public Accounts of Dáil Éireann (Privilege and Procedures) Act 1970 to be invalid on the grounds, *inter alia*, that it infringed Article 38.5 of the Constitution. The Supreme Court there followed with an ancillary order that the conviction and sentence in March 1971 had to be quashed because the prosecution of Mr. Páraic Haughey relied on an unconstitutional foundation. The powers of the Oireachtas Committee were invalid and therefore the investigation was invalid. There is a critical difference in the position of the Plaintiff – the prosecution and trial were concluded with statutory powers which remain valid and unchallenged. The Plaintiff only challenges the adducing of specific evidence at his trial. In these proceedings the Plaintiff confines his prayer for reliefs to declarations which will allow him to advance the argument at his appeal hearing about excluding particular evidence of attribution. In summary, the common law rules of evidence are procedural as opposed to being substantive. It does not automatically follow that telephony data retained and accessed contrary to EU law which was used by the prosecution will lead to the quashing of the conviction for murder.

4.16 There is a marked difference between the effect of a declaration of inconsistency with the Constitution or EU law on a substantive edifice like the establishment of an Oireachtas Committee to the effect of a declaration on procedural rules in criminal trials. It is worth adding in this context that the rules of evidence vary among Member States in prosecutions for murder. This means that there are no common means of determining the effects of an EU law breach on evidence rules.

4.17 Depriving every person whose rights were allegedly violated by the application of the 2011 Act of the possibility of seeking a remedy is a serious step which runs contrary to the role of the courts. Such a step requires unassailable evidence that the harm resulting from incompatibility *ab initio* justifies the restriction of the right of access to the court and the right

to an effective remedy. The consequences are not clear and should be determined on a case-by-case basis. The trial Judge, as in the prosecution of the Plaintiff, is best placed to determine whether it is fair and right to adduce specific evidence.

4.18 Furthermore, some cases may involve a significant breach to the right to respect for private life under EU and ECHR law. Both the Advocate General and the ECJ in *Tele2* found that retained data provides the means "*of establishing a profile of the individuals concerned*" and "*is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance*." (paras. 99-100). *Murphy v. AG*, on the other hand, involved pure economic loss.

4.19 The Court concludes that the legal system in Ireland can allow for an orderly consideration of the retrospective effects of the declarations on the adducing of evidence in each case according to the particular circumstances presenting.

Suspended declaration

4.20 The Defendants submit that as a matter of EU law, a national court has jurisdiction to suspend the taking effect of any declaration of inconsistency of national law with EU law. They state that it would "*be entirely in harmony with the* [ECJ's] *case law to suspend the effects of any declaration of inconsistency in the circumstances of this case*".

4.21 Relying on *Kadi and Al Barakaat International Foundation v. Council of the European Union & Commission of the European Communities (Joined Cases C-402/05 P* and *C-415/05 P)* [2008] ECR I-6351 (***"Kadi"***), they request this Court to maintain the effects of the 2011 Act for a period in order to give the legislature an opportunity to amend the 2011 Act. In *Kadi*, the ECJ struck down a regulation imposing sanctions on the applicant but maintained the effects of the regulation for a period of three months in order to give the EU

legislature an opportunity to amend its legislation and in light of the serious and irreversible prejudice that could flow from annulment with immediate effect.

4.22 The Defendants also refer to the judgment of the High Court of England and Wales in *Liberty* delivered on 27th April, 2018, as an example of a Member State court adopting this approach to suspend effects. In that judgment, the State defendants had conceded that part of the legislation providing for access to data was incompatible with EU law (Part 4 of the IPA). Therefore, the High Court had to consider, *inter alia*, what was the appropriate remedy in circumstances where that part of the legislation was nonetheless operative and had not been amended. That Court noted that while it was well-established that any legislation which is inconsistent with directly effective EU law is ineffective to the extent of its incompatibility, there is no automatic rule that incompatible national legislation must be disapplied immediately. The following paragraphs from the Court of Appeal judgment at paras. 74-76 encapsulate the reasoning urged upon this Court:-

> "*74. Nevertheless, it seems to us that a fundamental question which has to be addressed in cases such as the present is: what exactly is the nature and extent of the incompatibility of national legislation with directly effective EU law? Sometimes, the incompatibility may consist of a provision in national legislation which can simply be ignored or regarded as overridden by the relevant norm of EU law. For example, if national legislation imposes a procedural threshold before a person can bring a claim in the Employment Tribunal of working for at least 16 hours per week (the sort of condition which there was in the* EOC *case* [*R v. Secretary of State for Employment, ex p. Equal Opportunities Commission* [1995] 1 AC1]*), the consequence of incompatibility with directly effective rights in EU law (such as the right not to be discriminated against) may simply be that the procedural threshold in national law is to be ignored and will not operate as a matter of law to prevent the claim being*

properly lodged in the Employment Tribunal. That action by a court or tribunal does not on analysis require any order to be made by it. Often the court will make an appropriate declaration but it may be that the relevant court or tribunal has no jurisdiction to make even a declaration. It will still be under a duty to disapply the incompatible national legislation. The court or tribunal simply regards the rule of national law as being ineffective to the extent of its incompatibility with directly effective EU law.

75. In the present case, however, in our view, the nature and extent of the incompatibility with EU law which the Defendants accept does not go that far. As a matter of principle, there is nothing in EU law which prevents a Member State from having in place national legislation which permits the retention of data (to meet the crime objective) along the lines of the 2016 Act. The incompatibility which has been identified by the CJEU and is accepted by the Defendants consists of two failures to have certain safeguards in the legislation concerned. Correcting those failures will require positive steps to be taken by way of amending legislation. On any view, that was always bound to take some time. We are unable to reach the view that, from the moment when the incompatibility was pronounced by the CJEU or when it was acknowledged by the Defendants in this country, the national legislation had as a matter of absolute obligation to be disapplied immediately. That would, as Mr Eadie QC submitted on behalf of the Defendants, be a recipe for chaos.

76. These are deep constitutional waters, in which the courts of this country have been and still are feeling their way. In our judgement, the appropriate and principled approach is for the Court to allow both the Government and Parliament a reasonable amount of time in which they have the opportunity to enact national legislation to correct the defects which exist and which are incompatible with EU law. That was, as

we understand it, implicit in the Claimant's own approach to this important and difficult issue as the case was originally put. We consider that was a sensible approach as a matter of principle."

4.23 In brief, the Defendants effectively contend that chaos will reign if the declaration made by this Court has the usual retrospective effect.

The Plaintiff's arguments

4.24 Counsel for the Plaintiff confined his reply to challenging the contention that the ECJ jurisprudence on temporal effects allows this Court to suspend the effect of EU law at a national level. He mentioned that the ECJ has itself not imposed a temporal limitation on the declaration of invalidity given in *Digital Rights* and was not asked to do so in *Tele2*. Further, neither of the parties before this Court have requested a reference to the ECJ about the temporal effect at EU level of the declaration of invalidity in *Digital Rights*.

4.25 The overall position of the Plaintiff is that the Defendants, by seeking a temporal limitation or suspension, merely wish to deprive the Plaintiff of his ability to argue the question about the admissibility of the telephony data for the 407 phone in the Court of Appeal.

Recent case law

4.26 There has been recent jurisprudence from the Supreme Court regarding the possibility of suspending declarations of unconstitutionality. This was discussed in:-

(i) *N.H.V. v. Minister for Justice & Equality* [2017] IESC 35; [2018] 1 I.R. 246 **("*NHV*")**;

(ii) *Persona Digital Telephone Limited & Another v. Minister for Public Enterprise & Others* [2017] IESC 27 (Unreported, Supreme Court, 23rd May, 2017) **("*Persona*")**;

(iii) *C. v. Minister for Social Protection & Ors* [2017] IESC 63; [2017] 2 I.L.R.M. 369; and

(iv) *C. v. Minister for Social Protection & Ors* [2018] IESC 57 (Unreported, Supreme Court, 28th November 2018).

4.27 In the first *C.* judgment , MacMenamin J. reflected that the Supreme Court had in *NHV* and *Persona* addressed the question of constitutional remedies with suspending type effects. The parties were given an opportunity to make further submissions.

4.28 In the second *C.* judgment delivered on the 28th November 2018, O'Donnell J. (Clarke C.J., McKechnie J. and O'Malley J. concurring), declared that the courts did have jurisdiction to give a suspended declaration. However, he noted that "[t]*he precise circumstances in which* [this is] *appropriate … is … a matter to be considered carefully, cautiously, and on a case by case basis, and will be exceptional*." (para. 21).

Decision on suspended declaration

4.29 These recent Supreme Court judgments show that the law on suspending declarations is emerging. At the very least it is exceptional. It is determined on a case by case basis and, as discussed below, it is not appropriate in this case.

4.30 The legislative process following the Murray Review has begun. There is a need to exercise judicial restraint and give the respect which this Court owes to the executive and the Oireachtas. In addition, no good reason has been offered to interfere with what has occurred and is occurring according to the chronology. In other words, the Court is reluctant to

interfere with the timetabling by the Oireachtas for the proposed legislation as outlined in the chronology.

4.31 Insofar as the High Court of England and Wales saw fit to accommodate its legislature in *Liberty* earlier this year, Ireland through *Murphy v. AG* has established a *modus operandi* and *modus vivendi* in the "*constitutional waters*" with which England and Wales "*are feeling their way*".

4.32 Taking all of this into account, the Court accepts the submission of Counsel for the Plaintiff that "*the writing has been on the wall for the Act for some very considerable time now*". The Defendants have long been on notice of the defects in the legislation. Even if the Defendants claim that the law was left unclear after the judgment in *Digital Rights* in April 2014, the Murray Review in April 2017 concluded that "*many of the features of the data retention scheme established by the Act are precluded by EU law*." (para. 401). Mr. Justice Murray recommended that "*consideration be given to the extent that, if at all, statutory bodies should, as a matter of policy, continue to access retained communications data under the provisions of the 2011 Act pending the final resolution of issues pertaining to the status of the Act and/or any amending legislation conforming with EU law and obligations under the ECHR*." (para. 401).

4.33 Finally, the primacy of EU law is the foundation for this judgment and loomed large throughout the entire hearing of these proceedings. One of the major obstacles affecting the position of the Defendants is that Ireland and its courts have no option but to apply EU law which prohibits "*general and indiscriminate retention*" and access which is not authorised by a court or an independent administrative authority in accordance with law. It is a well-established principle that where national law conflicts with EU law, the organs of the Member States are under a duty to disapply their national law. The ECJ in *Simmenthal* stated:-

"*… a national court which is called upon, within the limits of its jurisdiction, to apply provisions of Community law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for the court to request or await the prior setting aside of such provision by legislative or other constitutional means.*" (para. 24).

4.34 Furthermore, the ECJ has stated that:-

"*Any provision of a national legal system, including provisions of a constitutional nature, and any legislative, administrative or judicial practice which might impair the effectiveness of EU law by withholding from the national court having jurisdiction to apply such law the power to do everything necessary at the moment of its application to set aside national legislative provisions which might prevent EU rules from having full force and effect are incompatible with those requirements, which are the very essence of EU law … This would be the case in the event of a conflict between a provision of EU law and a national law, if the solution of the conflict were to be reserved to an authority with a discretion of its own, other than the court called upon to apply EU law, even if such an impediment to the full effectiveness of EU law were only temporary.*" (*Kernkraftwerke Lippe-Ems GmbH v. Hauptzollamt Osnabrück (Case C-5/14)* ECLI:EU:C:2015:354, para. 33).

4.35 Neither the EU legislature nor the ECJ have provided for a limited temporal effect in accordance with the Charter for the declaration of invalidity in *Tele2*. No Member State court can usurp the competences of the EU legislature or the ECJ. This Court also has a lingering concern that any suspension of EU law by this Court as might be confirmed in some way by a court of final appeal in Ireland could render the State liable for reprimand and sanction.

4.36 In *Köbler v. Austria (Case C-224/01)* E.C.R. I-10239, the ECJ applied the principle according to which Member States are liable for damages caused to individuals as a result of infringements of EU law, to infringements stemming from a decision of a court adjudicating at last instance (para. 50). The ECJ stressed the condition that it be a court of last instance as this is "*the last judicial body before which individuals may assert the rights conferred on them by Community law*." (para. 34). The test for finding a Member State liable for reparation requires that "*the rule of law infringed must be intended to confer rights on individuals; the breach must be sufficiently serious; and there must be a direct causal link between the breach of the obligation incumbent on the State and the loss or damage sustained by the injured parties*." (para. 51) The ECJ held that an infringement of EU law will be sufficiently serious where "*the decision concerned was made in manifest breach of the case-law of the Court in the matter*" (para. 56).

5. CONSTITUTION

Introduction

5.1 Both sides relied on the Constitution to support their positions. It is common case that an analysis of the constitutional issues raised at the hearing is unnecessary if the Plaintiff is granted an effective remedy. This Court is not satisfied that a declaration of inconsistency with EU law by virtue of the reasoning applied under the remedies part of this judgment is substantially inferior to a declaration of invalidity having regard to the provisions of the Constitution. In that way, one may understand how the order of discussion in this judgment has come about.

5.2 It may be useful at some stage in the future to identify some of the key constitutional points which were advanced in submissions.

Article 29.4.6°

5.3 There is no controversy that after the declaration of invalidity in respect of the 2006 Directive by the ECJ in *Digital Rights* that the 2011 Act is not immune from constitutional challenge by virtue of Article 29.4.6° of the Constitution which provides:-

> "*No provision of this Constitution invalidates laws enacted … by the State, before, on or after the entry into force of the Treaty of Lisbon, that are necessitated by the obligations of membership of the European Union … or prevents laws enacted, … by –*
>
> *(i) the said European Union …*
>
> *from having the force of law in the State*."

Qualified Right of Privacy

5.4 It is further not in dispute that the unenumerated right to privacy of the Plaintiff under Article 40.3.1° of the Constitution is not an unqualified right. "*Its exercise may be restricted by the constitutional rights of others, by the requirements of the common good and is subject to the requirements of public order and morality*" (Hamilton P. in *Kennedy v. Ireland* [1987] I.R. 587 at 592).

Presumption of Constitutionality

5.5 The Plaintiff bears the onus of proving that the 2011 Act is unconstitutional (*Ryan v. Attorney General* [1965] I.R. 294 at 353). Nothing was conceded about the lack of proportionality of acts undertaken pursuant to the 2011 Act as they affected the Plaintiff. The evidence led before this Court at the request of the Defendants was directed to an assessment of the appropriateness, necessity and proportionality of the enactment and then the operation of the relevant provisions of the 2011 Act. The Plaintiff has not established that access to the relevant telephony data was inappropriate, unnecessary or disproportionate even though the

retention was not valid by virtue of EU law. While complaining about the loose statutory safeguards for access, the Plaintiff principally argues that the retention provisions of the 2011 Act are not rationally or proportionally connected to the objective sought to be achieved by the legislation. He contends that the indiscriminate and arbitrary regime affects every citizen and should not be permitted because otherwise every innocent person can fall into the category of being a suspect. Effectively he adapts many of the points considered by the ECJ in *Digital Rights* and *Tele2* to bolster his claim in this regard.

5.6 There is also the unopposed proposition articulated for the Defendants that any attempt at transposing "*the requirements of the Charter to the Constitution*" is ill-founded because "*the Irish Superior Courts have exclusive jurisdiction to define the scope and limits of the rights protected under the Constitution which have been guaranteed over many decades long before the Charter was proclaimed or given legal effect*". Further, "*…the logic that informed the* [ECJ] *analysis does not necessarily apply in precisely the same way to constitutional analysis*".

Position of the Defendants

5.7 The Defendants submit that anyone who claims that a statute is repugnant to the Constitution must take care to construe the right asserted in the context of the Constitution as a whole to give its true evaluation and standing in the hierarchy of rights. He or she must then show how, in light of that analysis, the particular statute is both an interference with that right and one which is incapable of justification.

5.8 They also rely upon the principles set out by Costello J. in *Heaney v. Ireland* [1994] 3 I.R. 593 at 607, when requesting the Court to consider the proportionality test in this constitutional challenge:-

"*The objective of the impugned provision must be of sufficient importance to warrant overriding a constitutionally protected right. It must relate to concerns pressing and substantial in a free and democratic society. The means chosen must pass a proportionality test. They must:-*

(a) be rationally connected to the objective and not be arbitrary, unfair or based on irrational considerations;

(b) impair the right as little as possible, and

(c) be such that their effects on rights are proportional to the objective: Chaulk v. R. [1990] 3 S.C.R. 1303 at pages 1335 and 1336."

5.9 The Defendants assert that the claim should concern the effect of the alleged unconstitutional measure and that the Plaintiff has not adduced evidence about effect. The Plaintiff, according to the Defendants, does not complain as to how any aspect of his private life was impacted by the impugned sections. He does not explain his sense of grievance about having been the subject of surveillance and he has not availed himself of the statutory complaints procedure.

5.10 The Defendants in resisting the challenge also:-

(i) outline how they await a description by the Plaintiff of the alleged significant impairment of his constitutional right to privacy and an explanation for his failure to avail of the statutory procedure for complaints under s. 10 of the 2011 Act;

(ii) differentiate between the tapping and interception of communications as mentioned in *Kennedy v. Ireland* [1987] I.R. 587 and *Schrems v. Data Protection Commissioner* [2014] 3 I.R. 75;

(iii) justify the enabling of the prior review of disclosure requests to the TLU by comparing it with provisions for more intrusive measures of searching a home, constant surveillance and interception of communications;

(iv) use the complaints procedure presently presided over by a Circuit Court Judge (s. 10 of the 2011 Act), the duties of the designated High Court Judge (s. 12) and the role of the DPC as assurances for the subjects of telephony data requests.

Damache

5.11 Both parties in support of their positions cited *Damache v. DPP* [2012] 2 I.R. 266, which accepted the Court of Criminal Appeal's literal interpretation in *DPP v. Birney* [2007] 1 I.R. 337 of "*Superintendent*" without the adjective "*independent*" to render s. 29 of the Offences Against the State Act 1939 unconstitutional. This may cause problems for the application of the double construction rule and the presumption of constitutionality in a challenge to the data access provisions of the 2011 Act. On the other hand, it may be possible depending on the circumstances which will involve this thorny issue in the context of accessing data to rely on the approach taken by Charleton J. in the Supreme Court when he stated at para. 246 in *CRH plc. & Ors v. Competition and Consumer Protection Commissioner* [2018] 1 I.R. 521:-

> "*The Constitution, in contemplating the attainment of 'true social order', as recognised in the Preamble, could hardly extend to the planning of crime the protection of a specific right that is recognised because of the legitimacy of people being enabled to retreat from public notice*…."

Comments by this Court

5.12 It is manifestly clear that embarking on a constitutional analysis will lead this Court into very fresh and much "*deeper constitutional waters*" that involve the increasing worries about the surveillance of citizens. The ECtHR's recent judgments and the US Supreme Court opinion in *Carpenter* (identified in the chronology) indicate the focus of preoccupation in those courts on the accessing of cell site location information (encompassing telephony data) by State authorities. Chief Justice Roberts noted how cell phone services are now such a "*pervasive and insistent part of daily life*" before commenting that "*… in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements Smith, 422 U.S., at 745.*" (p. 17).

5.13 In 1949, George Orwell published the dystopian novel *1984* which portrays a dehumanizing and unpleasant society that resonates with the feared abuse of 21st century surveillance. The prospect of anything resembling such a society prompts an *obiter* statement that organs of the State should tread carefully when trenching upon the dignity and privacy of the human person in the sphere of telephony data retention and access. Just as crime is required to be investigated, there should be transparency of use or abuse of power. Notification, supervision and enforceable sanctions are means to limit abuses. The chilling effect on privacy and the rights of free expression and association by actual, feared and mandatory surveillance cannot be underestimated.

5.14 Following upon this train of thought, it appears apposite to quote the first paragraph of the Advocate General's opinion in *Tele2* in order to elaborate:-

> "*1. In 1788, James Madison, one of the authors of the United States Constitution, wrote: 'If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the*

great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.'"

5.15 Lastly, it is proper to acknowledge the many publications submitted to this Court which enlightened the Court about the extent of data gathering and use within the past few years. The material included a reference to a book entitled *Data and Goliath* by Bruce Schneier (2015 hardback). At p. 97 the author commented in a way which is striking because it echoes 21st century trepidation about modern surveillance:-

> "(Philosopher and founder of utilitarianism) *Jeremy Bentham's key observation in conceiving his panopticon was that people become conformist and compliant when they believe they are being observed. The panopticon* [a watchman observes occupants without the occupants knowing whether they are being watched] *is an architecture of social control. Think of how you act when a police car is driving next to you, or how an entire country acts when state agents are listening to phone calls. When we know everything is being recorded, we are less likely to speak freely and act individually. When we are constantly under threat of judgment … we become fearful that … data we leave behind will be brought back to implicate us …. In response, we do nothing out of the ordinary. We lose our individuality, and society stagnates. We don't question or challenge power. We become obedient and submissive. We're less free*."

5.16 As indicated at the beginning of this judgment (paras. 1.18-1.19), there is a limit to the review which this Court can undertake. The availability of private surveillance whether through CCTV, use of social media, or other artificial intelligence facilities on devices for learning, interacting or entertainment fall outside the scope of this Court's consideration. Lastly, the enactment of the 2011 Act is premised largely but not exclusively on the invalid

2006 Directive and in that way there is an additional reluctance to embark on areas of legislation policy with which the Plaintiff is not concerned.

5.17 Lest there be any misunderstanding or inference, the Court reiterates that the Plaintiff has not established for this Court that the actual operation of the 2011 Act from retention in November 2011 to the date of disclosure in October 2013 for telephony data of the 407 number was inappropriate, unnecessary or disproportionate.

5.18 The grounds of appeal by the Plaintiff to the Court of Appeal from his conviction refer to the potential inadmissibility of evidence at his trial by reason of the subject of the declarations which this Court will make in early course. The trial Court ruled that it was admissible and the Plaintiff has exercised his right to appeal that ruling.

5.19 The chronology at para 2.27 identifies the McCarthy ruling, the Court of Appeal judgment in *DPP v. Flynn*, the White ruling and the second White ruling in order to highlight that each trial relying upon mobile telephony data evidence must consider the facts of each case before determining the admissibility of the evidence.

Conclusion

5.20 The Court will not make a declaration concerning the alleged repugnancy of sections 3 and 6 of the 2011 Act with the Constitution. The discussion of the invalid 2006 Directive together with the referred legislation from England and Sweden that were considered in *Tele2* do not require this Court to determine the constitutionality of the impugned sections. That does not mean that the in-depth analysis by the ECJ cannot influence the reasoning to be adopted if this Court could decide or was obliged to decide on the Plaintiff's claim of invalidity having regard to the Constitution relating to retention and access.

5.21 On the other hand, it follows from the extensive consideration and subsequent determination of each of the issues raised that declarations can be made. One of the principal

purposes of this judgment, which might not ordinarily be so extensive when discrete declarations can be made, is to adjudicate as far as possible upon the submissions made bearing in mind the many strands which could lead to differing results.

5.22 Before finalising the terms of the declarations, it appears that one issue has not been discussed and I will afford an opportunity to the parties to address same if they are not in agreement. The Court indeed proposes to make declarations about the inconsistency of ss. 3(1), 6(1) and 7 of the 2011 Act with EU law. However, if such declarations are made, is there a necessity to make a declaration pursuant to s. 5 of the ECHR Act concerning the limited incompatibility of ss. 6(1) and 7 of the 2011 Act with the right to respect for private life under Article 8 of the ECHR?

5.23 The Court has prepared draft declarations which it will circulate following delivery of this judgment for the purpose of inviting final submissions about the exact terms of a perfected order and the necessity for a declaration pursuant to s. 5 of the ECHR Act. In this regard it is noted that the effect of a declaration under s. 5 of the ECHR Act appears less than that available under EU law. Section 5(2) of the ECHR Act provides that a declaration "*shall not affect the validity or continuing operation or enforcement of*" those provisions in the 2011 Act and "*shall not prevent a party*" to these proceedings "*from making submissions…*" to the ECtHR. Indeed, s. 5(3) prescribes an obligation for the Taoiseach to lay a copy of any "*order containing a declaration of incompatibility … before each House of the Oireachtas within the next twenty-one days on which that House has sat after the making of the order*". There has been little if any discussion about exercising restraint when making declarations under the ECHR Act like the restraint applied when making declarations of repugnancy to the Constitution where the issue between the parties raised can be determined otherwise. Bluntly, is there any practical purpose in making a declaration pursuant to s. 5 of the ECHR Act along the lines of the draft? Rather than the Court assume positions which may be taken,

the parties are invited to address the Court on a later and convenient date about this aspect before the final orders are made and perfected.

[i] While Article 10 of the ECHR and Article 11 of the Charter were raised in the pleadings, no arguments were advanced in relation to the right to freedom of expression. Therefore, this judgment does not consider those rights.